# антивирусы в корпоративной среде

крис касперски, no-email

**от качества антивируса во многом зависит надежность корпоративной сети. но какой из них выбрать? на рынке присутствует множество игроков: AVP, Dr. Web, Trend-Micro, Symantec, NOD32, McAfee, продукты которых мы тщательно протестировали на широком спектре потребительских характеристик, описав полученные результаты в настоящей статье.**

## *введение*

Антивирусы с точки зрения конечного пользователя представляют собой "черный ящик" качество которого (в отличии от прикладных программ) невозможно оценить "невооруженным глазом". Снаружи находится только интерфейс, а "движок" скрыт глубоко внутри и раскрывает свои возможности только при встрече с реальной заразой, что происходит далеко не каждый день. Причем, "популярные" вирусы, вызвавшие массовые эпидемии, на роль тестового "эталона" совсем не годятся, поскольку распознаются практически всеми антивирусами, даже самыми отсталыми. А вот полиморфный rootkit, упакованный новой версией упаковщика защищенных файлов, способны распознать лишь лучшие антивирусы, да и то далеко не со 100% степенью вероятности.

Как показывает практика, подавляющее большинство потребителей (в том числе и корпоративных) в выборе антивируса руководствуется отнюдь не техническими характеристиками последнего, а личной симпатией (антипатией) к конкретному вендору. Очень часто приходится слышать утверждения в стиле: "мы используем продукт XXX от компании YYY, вот уже пять лет полет нормальный — вирусов нет". Так, может быть, это не вирусов нет, а просто антивирус такой слепой, что их не видит?! Ведь далеко не каждый вирус разрушает данные, поскольку это демаскирует его. Он может годами сидеть в информационной среде, занимаясь шпионажем или открывая back-door для удаленного управления системой, не вызывая и тени подозрений.

С другой стороны, антивирус, "ругающийся" на все файлы подряд (даже совершенно безобидные, как, например, стандартный "Калькулятор", упакованный широко распространенным упаковщиком UPX) еще хуже, поскольку создает атмосферу постоянной тревоги, вынуждая компанию тратить огромные средства (и время) на анализ ситуации и поиск черной кошки, которой нет, в черной комнате, которой никогда не существовало.

Вот какая, оказывается, непростая штука — выбор правильного антивируса!

## *а нужен ли антивирус?*

Во времена господства Windows 9x необходимость антивирусов никем не оспаривалась и тогда они являлись своеобразным "костылем", ликвидирующим наиболее слабые стороны операционной системы, а именно — катастрофическую незащищенность. В Windows 9x любой исполняемый файл имеет доступ ко всем ресурсам, в том числе и возможность незаметно устанавливать драйвера, переходя из прикладного режима на уровень нулевого кольца и встраиваясь в цепочку между оборудованием и операционной системой, скрывая от последней факт своего существования.

С приходом Windows NT/W2K/XP все изменилось. NT изначально проектировалась как защищенная операционная система, поддерживающая разделение привилегий и при правильно настроенной политике безопасности, вирус просто не может внедряться ни в какие исполняемые объекты, а потому оказывается нежизнеспособен.

Время глобальных вирусных эпидемий уже прошло (см. рис. 1). Даже почтовые черви, достигнув пика своей активности в 2003 году, к середине 2006 года сократили свою популяцию более чем в десять (!) раз. Зато приобрели большую актуальность целенаправленные атаки и rootkit'ы. Создание вирусов из мальчишеского хобби превратилось в бизнес и туда хлынули деньги, причем весьма приличные, надо сказать. Стоимость одного "заказного" вируса в зависимости его качества колеблется от $500 до $10.000, но даже серийные поделки редко опускаются ниже $100 – $500.

Антивирусы испытывают огромные трудности с детектированием неизвестным им вирусов, и даже мощный эвристический анализатор — плохой помощник, поскольку, заказчик (как правило) проверяет купленный вирус на самых последних версиях антивирусов и если хотя

бы один из них распознает заразу, вирус отправляется на доработку. В антивирусные базы попадают лишь небольшой процент вирусов, внедренных в программы, выложенные для всеобщего доступа на серверах типа www.download.ru. Из тысяч пользователей, скачавших программу, найдется по крайней мере один толковый специалист, владеющий отладчиком и распознающий вирусов методом "ручной работы". Однако, использовать программное обеспечение, полученное из ненадежных источников, категорически небезопасно! Даже если никаких вирусов там не окажется, неграмотно написанный инсталлятор вполне может обрушить систему или создать другие неприятности, так что в контексте корпоративного сегмента, эту проблему можно вообще не рассматривать.

Вирусы, основанные на общем "ядре", имеют хорошие шансы попасть в антивирусные базы (пускай и не сразу, а по прошествии довольно длительного времени). Нечестные на руку хакеры, вместо написания вируса с "нуля" под конкретный заказ, используют свои (или чужие) старые наработки, в результате чего, часть кода дублируется во всех вирусах, и один "засветившийся" вирус "палит" всех остальных. Однако, если уже известный антивирусу вирус упаковать новой версией упаковщика исполняемых файлов, то он в высокой степенью вероятности окажется необнаруженным. Разработчики упаковщиков, в борьбе с хакерами, ломающими программы, всячески препятствуют автоматической распаковке, вынуждая создателей антивирусов поддерживать множество статических упаковщиков, каждый из которых затачивается строго под "свою" версию упаковщика, причем, реализовать распаковщик намного сложнее, чем добавить очередную сигнатуру в базу. На это могут уйти десятки дней, в течении которых пользователи антивируса окажется совершенно беззащитны перед атакой.

С rootkit'ми дела обстоят еще хуже. Грубо говоря, rootkit'ы это вирусы, построенные по технологии Stealth. Попав на целевой компьютер они перехватывают ряд системных вызовов, маскируя факт своего присутствия на машине. В общем случае, антивирусы не способны обнаруживать активные rootkit'ы и все, что они могут – воспрепятствовать новым заражениям. То есть, если rootkit проник на компьютер прежде чем пользователь получил соответствующее обновление, антивирус его не увидит!!! Очевидно, что несерийные rootkit'ы, написанные специально для целенаправленной атаки на данную систему, антивирусами не обнаруживаются в принципе!

Ситуация кажется безнадежной, но… на самом деле, rootkit'ы отнюдь не всемогущи и большинство из них использует для своего распространения дыры в операционных системах и/или прикладных приложениях. Своевременная установка заплаток снижает риск успешной атаки в десятки раз! А если добавить сюда правильную настройку системы разграничения доступа, то у rootkit'а, независимо от способа его распространения, просто не хватит привилегий для проникновения в систему!

Важно понять, что антивирус — не панацея. Это всего лишь одних из элементов комплексной защитной системы, причем далеко не центральный ее компонент.

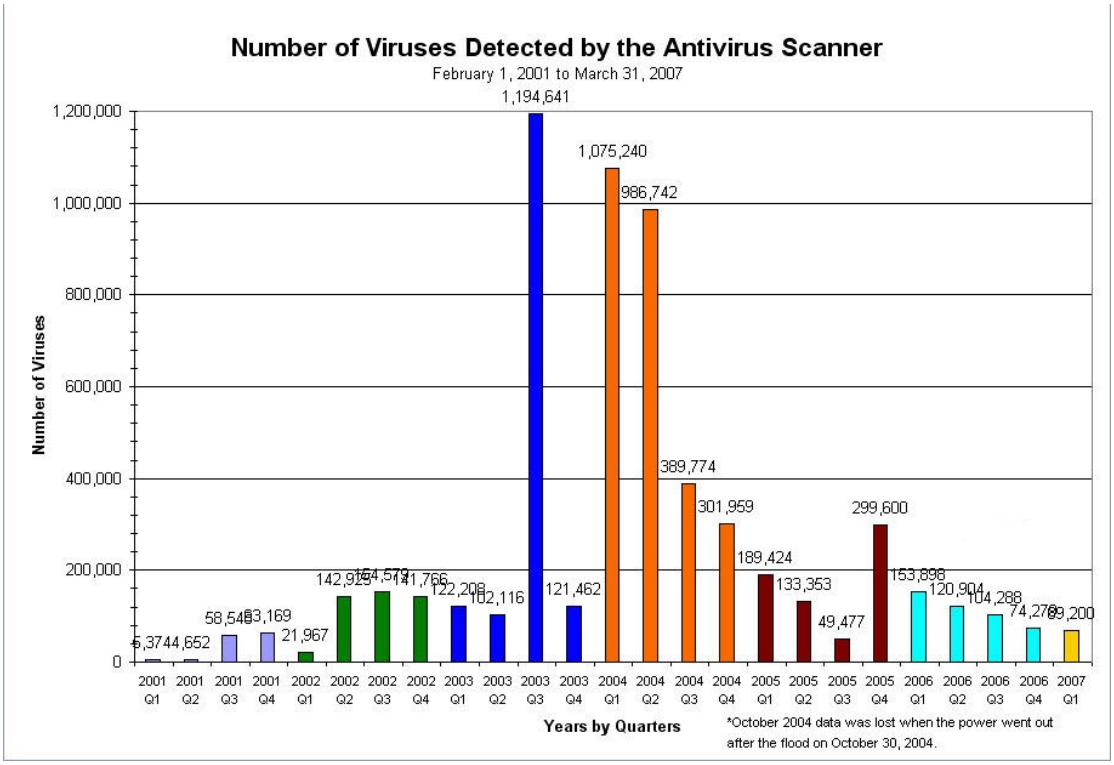


**Рисунок 1 активность почтовых червей (по данным UH Information Technology Services — ITS, http://www.hawaii.edu/antivirus/emailscanner.html)**

## *производительность*

Быстродействие — одна из важнейших характеристик антивируса. Мало кто хочет расплачиваться падением производительности за возросшую безопасность (тем более, что, как было показано выше, польза от антивирусов довольно сомнительна). Поскольку, быстродействие антивируса зависит от множество факторов, определяемых как "анатомическими" особенностями антивируса, так и типом сканируемого файла, это существенно затрудняет выявление лидеров и отсайдеров.

Одни антивирусы (AVP, Dr. Web) распаковывают файлы на встроенном эмуляторе ЦП (виртуальной машине) и несут на своем борту сравнительно небольшой набор статических распаковщиков, в результате чего способы обрабатывать даже новые версии старых упаковщиков и упакованные файлы со слегка поврежденной структурой. Другие же (NOD32, Trend-Micro) имеют намного более слабую виртуальную машину и вынуждены таскать за собой огромный набор статических распаковщиков — очень быстро работающих, но, увы, "обламывающихся" с распаковкой даже при незначительной модификации упакованного вируса. Опять-таки, тут все зависит от того какие файлы мы обрабатываем. Если в тестовом наборе доминируют неупакованные файлы, то обе категории антивирусов покажут приблизительно одинаковый результат, однако, если подсунуть AVP большое количество файлов, для которых у него нет статических распаковщиков, а у NOD'a – есть, то NOD32 порвет AVP как тузик грелку, уходя в вертикальный отрыв с реактивным выхлопом.

Эвристический анализатор вообще не позволяет измерять свою производительность в естественных единицах. Дело в том, что глубина анализа задается не в машинных командах, а в… миллисекундах и если по истечению заданного промежутка времени антивирус не найдет ничего подозрительного, сканирование файла прерывается и он считается "здоровым" (чем с успехом пользуются создатели вирусов, вставляющие в начало своих творений циклы с большим количеством итераций). Естественно, чем больший промежуток времени отпущен эвристическому анализатору, тем ниже его производительность (даже на здоровых файлах), но выше вероятность найти заразу.

Далее, если антивирус не выполняет полного сканирования файла, а всего лишь ограничивается проверкой окрестностей точки входа, производительность увеличивается в десятки (или даже сотни раз), но вместе с этим снижается качество детектирования.

Поскольку, алгоритм работы антивируса зависит не только от его конструктивных особенностей, но так же и пользовательских настроек (которые, в частности, позволяют задавать уровень глубины сканирования и т. д.) становится понятно, что сравнение производительности антивирусов совершенно ни о чем не говорит. Как минимум необходимо уточнить с какими настройками и на каком наборе файлов проводилось тестирование.

Плюс, разные антивирусы поддерживают различные форматы файлов (ведь вирусы могут сидеть не только в exe/dll, но и html, jpg, cur, ico и т. д.). Очевидно – чем больше форматов поддерживает антивирус, тем ниже его производительность.

Тем не менее, для получения общего представления о картине, ниже приводится диаграмма (см. рис. 2), подготовленная независимой тестовой организацией Virus Bulletin, на которой NOD32 демонстрирует поразительный отрыв от своих конкурентов (в частности, AVP отстает чуть ли не на порядок). И хотя условия тестирования явно не указывались (что делает невозможным воспроизведение эксперимента), личный опыт автора хорошо согласуется с представленными данными. AVP, действительно, самый медленный из всех антивирусов и полное сканирование всех файлов занимает значительное время и сильно загружает процессор, причиняя пользователю множество неудобств, в результате чего, антивирус сплошь и рядом отключается или же выбирается самый "легкий" режим сканирования (только exe/dll-файлы без всякой эвристики). Естественно, вероятность обнаружения заразы при этом существенно снижается.

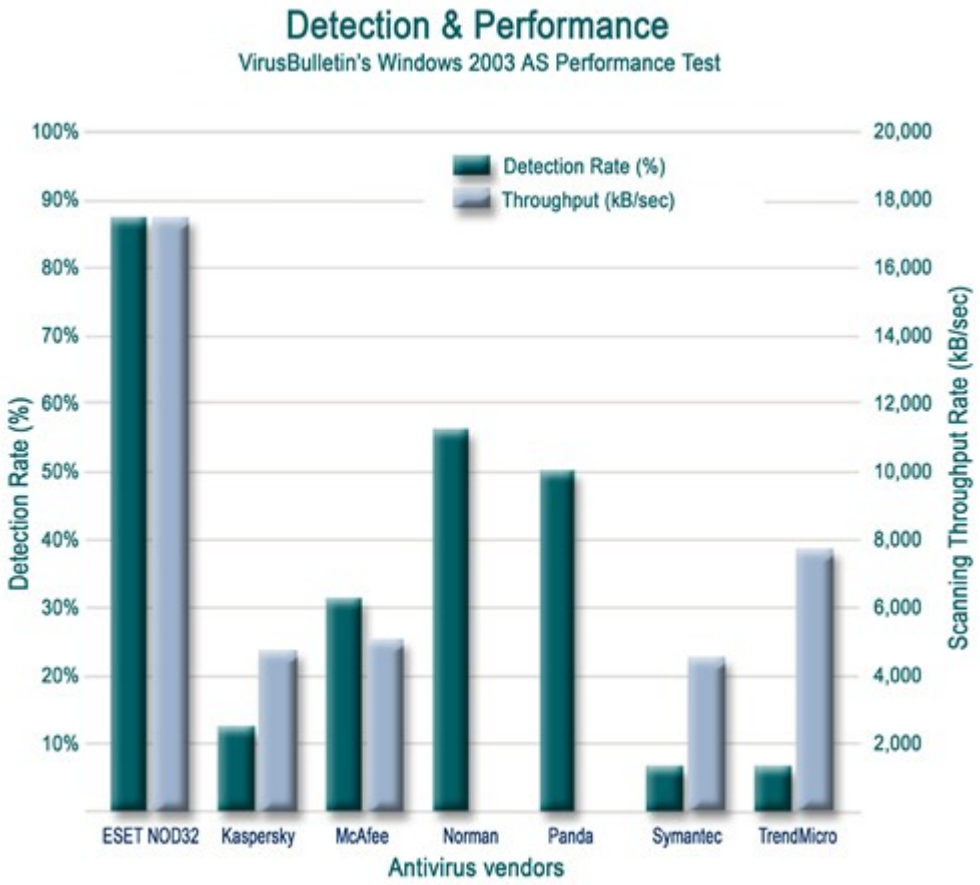


**Рисунок 2 производительность и качество детектирования различных антивирусов (по данным Virus Bulletin)**

## *качество детектирования*

Тестированием антивирусов занимаются многие компании, в том числе и независимые (например, Virus Bulletin – www.virusbtn.com), однако, сходимости в полученных результатах упорно не наблюдается. В частности, по данным Virus Bulletin, AVP отстает от NOD32 приблизительно в четыре раза, а по данным разработчиков антивируса Avira AntiVir (см. рис. 3), AVP даже слегка обгоняет NOD32 (98, 96% против 95,65%), аналогичного мнения

придерживается и тестовая организация AV Comparatives (97,89% против 96,71%) — http://www.av-comparatives.org/seiten/ergebnisse_2007_02.php.

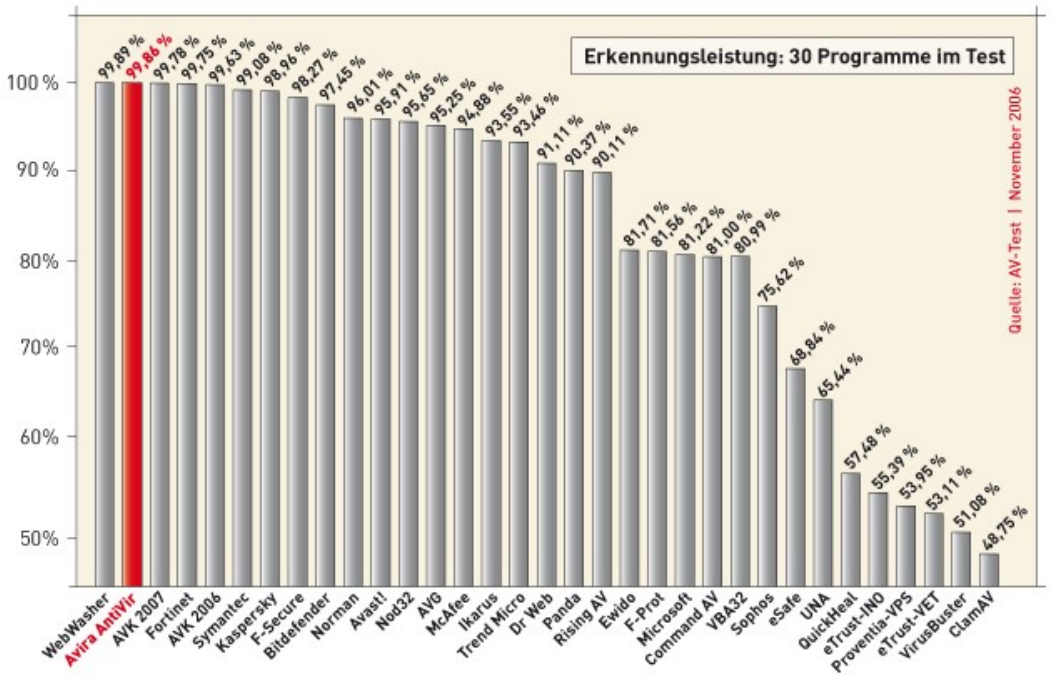


**Рисунок 3 качество детектирования различных антивирусов по данным разработчиком Avira AntiVir (http://www.avira.com/en/company_news/top_position_in_av-test_.html)**

Кому верить?! Увы, в сложившихся условиях верить нельзя никому и проценты распознанных вирусов на самом деле не проценты, а "попугаи". Какой в них смысл, если условия эксперимента не описаны, тестирование проводилось на закрытой коллекции вирусов по неизвестной методике?! Даже если предположить, что коллекция подобрана честно и максимально репрезентативно, а не просто позаимствована с CD-диска "10 тыс. вирусов", это ничего не меняет, поскольку совершенно непонятно за счет чего один антивирус оказывается лучше другого: толи проигравший органически не способен распознавать сложные вирусы (особенно, "обернутые" упаковщиками), толи просто не успел обновить свои базы. Учитывая, что вирусы появляются каждый день, а антивирусные базы обновляются отнюдь не синхронно, определенный случайный разбор в качестве детектирования заведомо неизбежен! Тем не менее, цифры, приводимые организацией Virus Bulletin (см. рис. 2) выглядят абсолютно неправдоподобными и никем не подтвержденными. Остальные тестеры не обнаруживают столь драматического разрыва между лидерами антивирусного рынка и разница между NOD32 и AVP редко превышает 1%-3%, причем чаще всего эта разница идет не в пользу NOD32.

Создатели AVP и Dr. Web размножают полиморфные вирусы в очень большом количестве (десятки тысяч экземпляров) и если хотя бы один из них не обнаруживается антивирусом, то это расценивается как дефект, требующий доработки, то есть качество распознавания в грубом приближении составляет 99,999%. При тех же обстоятельствах, NOD32 гарантированно пропускает до 10 экземпляров вируса, то есть распознает зараженный файл с вероятностью 99,9%. Важно подчеркнуть, что речь идет про распознавание _одного_ полиморфного вируса (неважно какого, любого достаточно сложного) и этот эксперимент может воспроизвести любой желающий. И не нужно думать, что 99,9% — это хороший показатель. 0,1% пропущенных вирусов — это _огромная_ величина!!! Допустим, в сети находится 100 компьютеров (локальная сеть небольшой организации) и вирус рассылает свои копии каждую минуту. Нетрудно рассчитать, через какое время все узлы окажутся зараженными нераспознаваемыми штаммами вируса!

Главный недостаток NOD32 (и большинства остальных антивирусов) в том, что он использует крайне примитивную технологию для распознавания полиморфных вирусов, а именно — сигнатурный поиск по маске. Часто для одного вируса требуется полсотни масок

(каждая из которых занимает отдельную запись в базе, создавая обманчивое впечатление, что NOD32 ловит полсотни разных вирусов), но и этого количества оказывается недостаточно для надежного детектирования.

Уникальность AVP и Dr. Web состоит в том, что для распознавания полиморфных вирусов они используют специальные алгоритмы, разрабатываемые с учетом специфики конкретного вируса. Это намного более трудоемкий, но вместе с тем и значительно более надежный путь, которым (пока) не воспользовался ни один западный разработчик. Что же касается сравнения AVP с Dr. Web'ом, то они представляют собой продукты приблизительно одинакового класса.

Так же необходимо помнить и о том, что некоторые антивирусы (и AVP в том числе) не распознают "дохлые" или неработоспособные вирусы, а так же программы, которые не были классифицированы как вирусы. Зато их может "находить" NOD32, хрюкая от радости, хотя на самом деле, никаких поводов для радости здесь нет. Хуже всего, что NOD32 вместо того, чтобы разбираться с некоторыми "навороченными" упаковщиками и протекторами, просто объявляют их вирусами, а это значит, что любой честный файл, обработанный таким упаковщиком, будет распознан NOD'ом как "зараженный"! И если NOD32 орет, а AVP молчит, то это еще не значит, что AVP – плохой антивирус.

Количество ложных срабатывай, вообще говоря, огромно. По данным Virus Total, при тестировании 11035 файлов на большой коллекции антивирусов, лишь 239 файлов были распознаны как зараженные всеми антивирусами, и в 10796 файлах заразу нашел по крайней мере один антивирус (см. рис. 4). Это наглядная иллюстрация того, что антивирусам доверять нельзя и у большинства из них качество детектирования находится на зачаточном уровне.

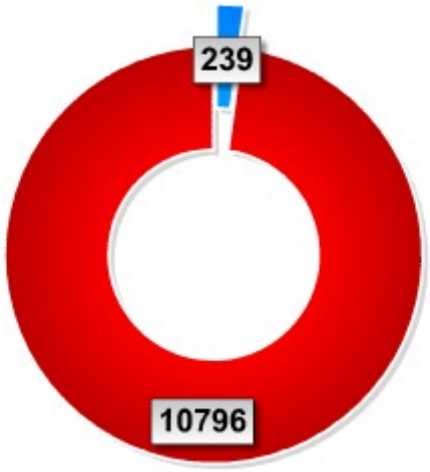


**Рисунок 4 статистика детектирования вирусов по данным Virus Total (http://www.virustotal.com/vt/en/estadisticasx)**

## *эвристический анализ*

Эвристический анализатор представляет собой мощное оружие, существенно осложняющее разработку вирусов, однако, доступность антивирусов позволяет "шлифовать" вирус, совершенствуя алгоритм маскировки до тех пор, пока его перестают распознавать все эвристические анализаторы, а потому, эвристика способа обнаружить лишь откровенно дилетантские вирусы, написанные "пионерами", даже не удосужившимися протестировать свое творение. Кстати говоря, таких вирусов в настоящее время подавляющее большинство, а потому эвристика представляет собой довольно полезную штуку.

По данным AV Comparatives самый мощный эвристический анализатор, значительно обгоняющий своих конкурентов, реализован в NOD32 (см. рис. 5), что совпадает с личным опытом автора. Эвристический анализатор NOD32 действительно поражает своей "проницательностью", особенно если учесть ее высокое быстродействие. AVP работает намного медленнее, да и качество у него не то. Bit Defender (и находится где-то посередине).

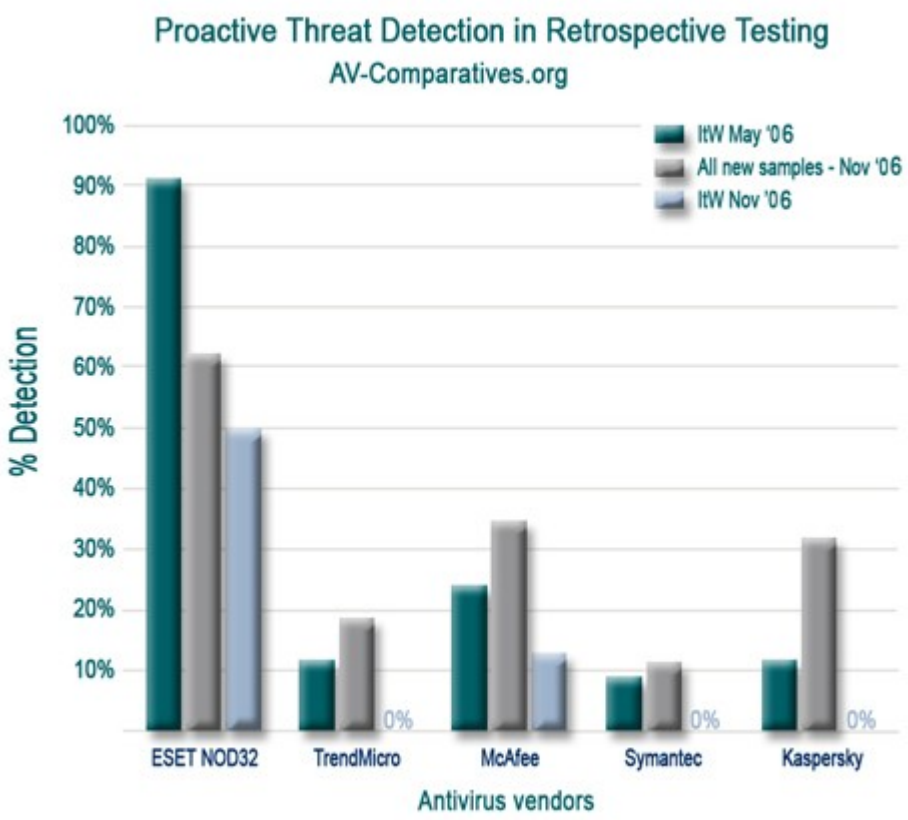


**Рисунок 5 процент распознанных вирусов эвристическими анализаторами различных антивирусов (по данным AV Comparatives – www.av-comparatives.org)**

## *proактивные технологии*

Еще во времена MS-DOS существовали антивирусные мониторы (от английского "monitor" – наблюдатель-перехватчик, не путать с устройством отображения видеоинформации), перехватывающие системные вызовы и выдающие запрос на подтверждение потенциально опасных операций (форматирование диска, запись в исполняемый файл и т. д.). Большой популярностью они не пользовались, зато отличались повышенной конфликтностью, легко обходились вирусами и конкретно раздражали пользователей, большинство из которых на все вопросы не задумываясь отвечало "yes".

С тех пор прошли десятки лет. Что изменилось? Ровным счетом – совершенно ничего! Мониторы превратились в "proактивные средства защиты", унаследовав все худшие качества своих предшественников, а именно:

а) proактивные защиты модифицируют ядро операционной системы, используя нетрадиционные приемы программирования (так называемые "хаки"), результатом которых становится многочисленные сообщения о критических ошибках и выпадения в BSOD. Чтобы покончить с этим раз и навсегда, в 64-битных редакциях Server 2003 и Висты Microsoft реализовала специальный механизм Patch-Guard, следящий за целостью ядра;

б) proактивные защиты легко обходятся старой доброй имитацией клавиатурного ввода или другими бесхитростными приемами, поэтому, они могут остановить только "пионерских" вирусов, написанных в расчете на "авось";

в) среднестатистический пользователь недостаточно квалифицирован, чтобы отличить "правильные" действия от "зловредных", а потому продолжает не задумываясь давить на "yes";

Короче говоря, если эвристический анализ "карман не тянет", то proактивные технологии из-за некорректно реализованного перехвата системных функций достаточно часто приводят к потерям данных, не говоря про зависания, перезагрузки и прочие мелкие неприятности, оборачивающиеся (в масштабах корпорации) крупными убытками.

## дыры в антивирусах

Антивирус может выступать не только "лекарством", но и объектом атаки, особенно если он содержит компоненты, работающие с администраторскими привилегиями и/или драйвера (а практически все антивирусы содержат их). Ошибки, допущенные разработчиками, позволяют хакеру в лучшем случае устраивать атаки типа "отказа в обслуживании", в же худшем — захватывать управление машиной. И это отнюдь не абстрактная теория, а суровая правда жизни, подтверждение которой можно найти, в частности, на www.securityfocus.com (равно как и любом другом ресурсе аналогичной тематике).

Как показывает статистика (см. рис. 6), самым дырявым оказывается Trend-Micro, однако, конкурирующие с ним продукты так же несвободны от дыр, поэтому, чем больше антивирусов установлено на компьютере, тем выше вероятность успешной атаки.

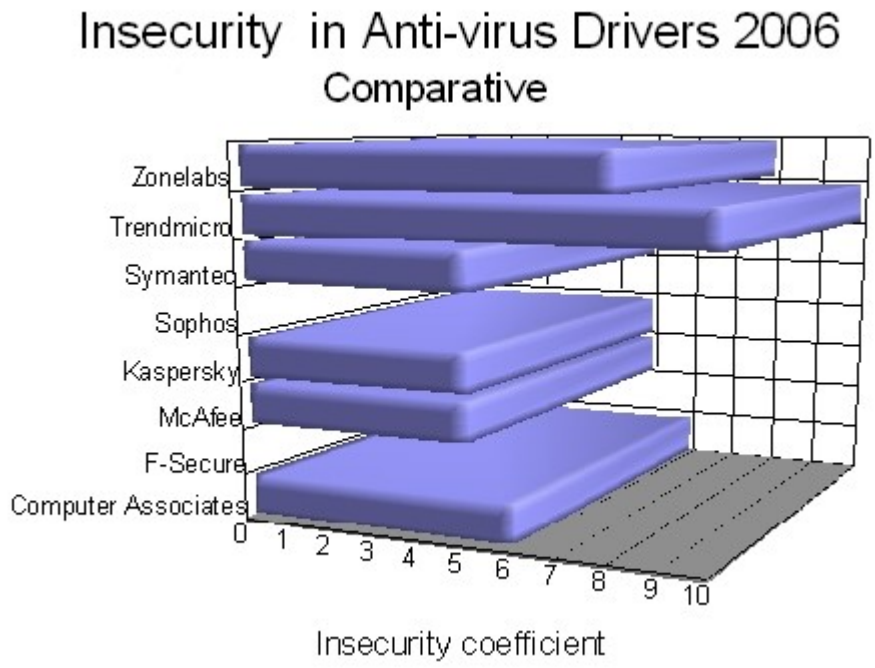


**Рисунок 6 средний коэффициент "инсекьюрности" различных антивирусов**

## заключение

Подведем итог: всем антивирусам присущи те или иные недостатки, поэтому, для достижения приемлемого качества детектирования разумно выбрать двух-трех лидеров рынка, основанных на принципиально различных "движках", например, NOD32 и AVP/Dr. Web, отключив рroактивные защиты, поскольку от них больше вреда, чем пользы.

Устанавливать более трех антивирусных пакетов не стоит — качество детектирования это уже не улучшит, зато увеличит количество ложных срабатываний, конфликтов и создаст реальную угрозу атаки на антивирус.