Говорят, что антивирус Dr.Web - продукт для домашних пользователей и серьезные компании его не используют.

Вебовцы отвечают – вот смотрите какие у нас клиенты, типа самые что ни есть корпоративные.

Еще бы нет друзья, ведь связи ДилогНауки (которые и сделали большую часть этих сделок) в государственных, около государственных и бывших государственных структурах коими являются очень многие крупные организации. Но увы из этого сектора Дрвеб вытесняют. Вытесняет Trend Micro например, вытесняет тот же Касперский

Вытесняют потому, что действительно нормальным решением для крупных компаний у дрвеб можно считать только линуксовые продукты. НУ чтоб не вызывать споры – предположим продукт для виндовых рабочих станций тоже отличный, хотя спорно☺ Комплексную защиту организации они дать не могут:

1.Очевидные пробелы в линейке: нет ексченджа, нет Лотуса, много чего нет

2.Возможности их админкита сильно уступают возможностям не только аналогичных инструментов Симантека Тренда и Макафи, но и того же Касперского. Приводить конкретные примеры не буду, возьмите мануалы и посмотрите.

А возможность работы на слабых машинах никто в вину не ставит доктору, просто это факт, что во многих компаниях нод32 и доктора используют исключительно на старых машинах.

Кстати есть такой миф, что доктор во многом такой легкий, потому что в нем нет многих функций которые необходимы для защиты от современных угроз☺ И не надо говорить, что они берут вирусбюллетени, объем коллекции этого уважаемого журнала смехотворен, сравните с объемами коллекции того же Климанти на av-comparatives.org. А про набор функций – поглядите-ка ClientSecurity от Симантека например, или на KIS6.0 (надеюсь новая рабстанция будет не хуже).

Мифы о степени защиты Антивируса Dr.Web

Говорят, что антивирус Dr.Web не проверяет критические области системы и объекты автозапуска, а именно они больше всего подвержены заражению.

Это миф. Сканер и SpIDer Guard (XP и Me) проверяют загрузочные сектора дисков, а также файлы автозапуска и лечат их в случае необходимости.

1. а какие области вы считаете критическими? и какие вы проверяете?
2. а какие объекты автозапуска вы проверяете?
3. а залоченные файлвы проверяете? Небось нет

Касперский под проверкой автозапуском понимаем получение ВСЕЙ системной информации обо ВСЕХ объектах, запускающийся при старте системы (в частности чтоб бороться с rootkits). Причем база объектов автозапуска у него обновляемая. Касперскаий лечит загрузочные сектора жесткого и съемных дисков в случае заражения вредоносным кодом путем перезаписи их сохраненными ранее чистыми копиями или при их отсутсвии- стандартной копией загрузочных секторов. Как у ДРвеба с этим?

Говорят, что антивирус Dr.Web "знает" мало архивов и поэтому уровень его защиты недостаточный.

Никто не говорит по-моему, что доктор Веб знает мало архиваторов и упаковщиков. НО знает он их меньше, чем другие. Доказано на деле
http://www.antimalware.ru/index.phtml?part=compare&anid=packs
А лечить в архивах Дрвеб не умеет.

Говорят, что антивирус Dr.Web недостаточно надежен, потому что не лечит вирусы в архивах.

Каждая антивирусная программа имеет собственную, уникальную концепцию построения защиты. Dr.Web действительно не лечит инфицированные вирусами файлы внутри архивов, но это совершенно не сказывается на надёжности Dr.Web, что подтверждается многочисленными наградами британского журнала Virus Bulletin - самой авторитетной в антивирусном вирусном мире награды.

Не надо смешить на вирусбюлютнем. Они там на зиповских архивах тестирую коллекции в несколько тыщ вирусов, эта награда доказаывает только то, что продукт обеспечивает минимально необходимый уровень защиты ниже которого опускаться очень плохо, ну совсем плохо.

Dr.Web прекрасно обнаруживает в архивах вирусы и при постоянно работающем мониторе SpIDer Guard у вируса нет шансов вырваться из архива и заразить систему. Более того, вряд ли любой другой антивирус может похвастаться тем, что он лечит любые архивы, в которых способен найти вирусы. Ведь для "лечения" архива надо не просто вылечить (или удалить) инфицированный файл внутри архива, надо ведь еще и перепаковать архив обратно, чтобы его содержимое было доступно пользователю. А в целом ряде случаев такая "перепаковка" просто невозможна без лицензирования алгоритма архивирования.

Ну здрасьте. Kaspersky лечит файлы в архивах ZIP, ARJ, CAB, RAR, LHA, Norton лечит в архивах ZIP, Trend Micro – ZIP, RAR2, LHA, a Panda лечит ZIP, ARJ, LHA. Лечат и перепаковывают ничего, нормально.

А по поводу не надо лечить это прекрасная идея – давайте удалим архив с доками над которыми месяц работали, там ведь вирус, ничего что труд на смарку – зато все безопасно. Вот чтобы такого не было и надо лечить.

Говорят, что в Антивирусе Dr.Web нет возможности задать область диска для контроля антивирусным монитором, чтобы повысить таким образом скорость работы.

С точки зрения разработчиков Антивируса Dr.Web подобный функционал - потенциальная уязвимость, а сама идея такой "выборочной" защиты - порочна, т.к. пользователю предлагает защищать всего лишь часть, вместо того, чтобы обеспечивать защиту целого - всей системы. Потенциально вирус может поразить любую область диска. Повышать таким образом производительность антивируса - за счет серьезного снижения безопасности - разработчики Dr.Web не готовы.

Ребята ну что вы говорите, вы же сами дальше пишите, что в докторе есть многочисленные настройки позволяющие убыстрить работу за счет снижения уровня безопасности. Это делается под ответственность пользователя.

Делаете так вы, делают так и другие, просто у других эта настройка еще более продвинутая. Зачем же тут говорить о порочности?

Ходит миф, что в Антивирусе Dr.Web нет возможности создания нескольких задач сканирования

Это неправда. Можно запустить несколько GUI-сканеров одновременно и одновременно же сканировать несколько разделов жёсткого диска. При этом будет достигнут значительный выигрыш во времени.

Очень удобно для пользователя и прекрасно скажется на быстродействии компа, просто мои поздравления.

Ходит миф, что в антивирусе Dr.Web нет возможности продолжить прерванное сканирование.

Это не так. Пауза при сканировании реализована в GUI-сканере.

Прямо с места, на котором остановилось сканирование? Че то по-моему вы лукавите.

Говорят, что в антивирусе Dr.Web нет временной приостановки защиты во время работы с ресурсоемкими пакетами

Это миф. У SpIDer Guard XP, SpIDer Guard Me, SpIDer Mail есть возможность временно приостановить мониторинг. Только в SpIDer Guard XP такая возможность доступна сразу, а в других перечисленных модулях такую возможность можно включить путем изменения настроек конфигурационного файла

О вот это очень удобно, особенно для домашних пользователей и админов большой сети. Что надо в разных местах чего-то где-то докручивать, вместо того, чтобы нажать правую кнопку на значке в трее и выбрать нужный подпункт меню

Кроме того у вас нельзя задать время отключения защиты, нельзя включить защиту при опред событии, пользователь забыл, что отключил, полез в инет и пиши пропало.

И вообще когда говорят о отсутствии у Дрвеба такой функции говорят еще о том, что хорошо бы была автоматическая возможность приостановить задачу сканирования, если процессор занят работой с другими приложениями

Говорят, что антивирус Dr.Web работает быстро потому, что не "узнает" макровирусы в офисных документах формата MS Office, а значит не проверяет такие документы.

Это миф. Dr.Web уже очень давно знает макровирусы во всех форматах документов MS Office. Более того, в эвристическом анализаторе есть алгоритмы, которые могут обнаруживать большинство никому ещё неизвестных новых макровирусов. Dr.Web является сильнейшим антивирусом по детектированию и лечению документов от макровирусов, а также вирусов, шифрующих документы пользователя с целью шантажа.

Ребята вы научились работать с макровирусами, очень хорошо с ними работает. Это правда. НО сильнейшие это крутовато, взгляните вот сюда: http://www.av-comparatives.org/seiten/ergebnisse_2006_02.php В графе макровирусы у многих процент обнаружения повыше будет.

Ходит миф, что в Антивирусе Dr.Web нет возможности применения выбранного действия ко всем видам угроз одного и того же типа

Я такого мифа не слышал.

Это неправда, такие настройки есть для каждого типа угроз:

- излечимые вирусы;
- неизлечимые вирусы;
- рекламные программы;
- программы дозвона;
- программы-шутки;
- потенциально опасные программы;
- программы взлома.

Говорят, что антивирус Dr.Web невозможно установить на уже зараженную машину

Это миф. Такая возможность есть и всегда была. Антивирус Dr.Web выгодно отличается от других аналогичных программ повышенной вирусоустойчивостью и способностью работать сразу на зараженной вирусом машине. Более того, Dr.Web можно запустить без установки в системе, непосредственно с любого внешнего носителя (компакт-диска или USB-памяти).

Да вы действительно реализовали механизмы противодействия активным процессам в памяти, что позволяет ставиться на зараженную машину. Насколько они эффективны не знаю- не проверял.

Ходит миф, что реализованная в антивирусе Dr.Web функция сканирования системы перед установкой антивируса не гарантирует установку программы на уже зараженную машину.

Это неправда. Большинство вирусов, находящихся в системе, могут быть обезврежены антивирусом Dr.Web при сканировании памяти и файлов автозагрузки уже в момент установки антивируса. Дополнительно, перед таким сканированием , в процессе установки антивируса базы можно обновить, что входит в процедуру установки. Таким образом, устанавливая антивирус Dr.Web, пользователь получает актуальные на момент установки базы, а не те, которые были записаны при комплектации дистрибутива.

Ребята ну как неправда. Ведь активные в памяти вирусные процессы могут активно противодействовать любым действиям антируса, в том числе обновлению Для успешной установки на зараженную машину нужно не предсканирование, а умение противодействовать активным процессам и механизмы самозащиты антивруса (чтобы процессы антивируса нельзя было вынести из системы.) Вы же сами отчасти реализовали эти механизмы, насколько успешно не могу судить.

Ходит миф, что в антивирусе Dr.Web нет возможности задавать исключения для сканируемых приложений

Это не так. Любой файл или папку можно исключить при желании из проверки в любом компоненте Dr.Web.

Ребята ходит миф что вы не можете исключить приложение из проверки, то есть исключить все что связано с процессами этого приложения. Файл и папку вы исключить можете, а вот приложение НЕТ.

Говорят, что в антивирусе Dr.Web нет поведенческого блокиратора

Это правда, но отчасти. Частями того, что можно назвать поведенческим блокиратором в антивирусе Dr.Web, являются:

- функция контроля вирусной активности в SpIDer Mail;
- функция контроля вирусной активности в SpIDer Guard Me;

Кроме того, Dr.Web обладает мощным эвристическим анализатором, который постоянно совершенствуется и в который постоянно вносятся изменения, в том числе через обновления вирусных баз.
Не достаточно эвристического анализатора, нельзя в режиме эмуляции эвристиком многие вредоносы отловить. А функции контроля вирусной активности не имеют никакого отношения к контролю реестра, целостности приложений (сами знаете о случаях внедрения и подмены вредоносами приложений) реализованных у Панды и Касперского, ну и Битдефендера по-моему. Кроме тот же Касперский умеет следить за процессами (за их действиями) и как только принимается решение, что процесс вредоносный – Касперский может откатить все изменения сделанные этим процессом и вернуть систему к незараженному состоянии.

Говорят, что в антивирус Dr.Web не проверяет HTTP-трафик "на лету".

Это частично правда. Полная поддержка проверки HTTP-трафик "на лету" реализована в бета-версии модуля SpIDer Gate (см . новость от 29.12.2005). SpIDer Gate своей функциональностью дополняет программы-брандмауэры (firewalls): последние закрывают уязвимости в системе, предотвращая возможные попытки злоумышленников произвести взлом и получить доступ к системе, но они не способны проверять файлы, загружаемые пользователем из Интернета (файлы, почта и т.д.), среди которых могут быть троянские программы, сетевые и почтовые черви, а также другие виды вредоносного кода.

Но и имеющийся SpIDer Guard также отлично сейчас справляется с такой поверкой, в том числе и с тем, что проходит через браузеры. Это, конечно, не полноценная проверка HTTP-трафика, но то вредоносное, что HTTP с собой приносит в систему мы пресекаем. SpIDer Gate, в основном, призван уменьшить нагрузку на систему, если единственным источником проникновения вирусов на компьютер является HTTP, позволяя в некоторых случаях отказаться от SpIDer Guard.

Всем понятно, что от вредоноса, который не создает в процессе своей жизни файл файловый монитор бессилен. Так что SpIDer Guard недостаточно именно поэтому вы делаете SpIDer Gate. Вот доделаете – поговорим.

Ходит миф, что в Антивирусе Dr.Web должен быть и файервол, т.к. он есть в некоторых других антивирусах.

Firewall (брандмауэр) и антивирус - слишком разные типы программ. Ни у кого ведь не придет в голову спросить директора танкового завода, почему его предприятие не строит боевые корабли, хотя и танк и корабль - средства обороны. Антивирус выполняет строго определенные функции, анализирует объекты на диске и в памяти компьютера, в то время как firewall анализирует пакеты, передаваемые по сети. Кроме того, ни в одном антивирусе нет firewall как такового. Другое дело, что в коробке с антивирусом часто можно увидеть и firewall того же производителя, но это не значит, что firewall встроен непосредственно в антивирус.

Антивирус может предлагаться совместно с брандмауэром для усиления защиты, но при этом брандмауэр не является обязательным компонентом антивируса. Антивирусы, брандмауэры, антишпионские программы - это только некоторые типы различных по функционалу программ, занимающиеся защитой информации.

Ребята еще со времен нимды сасера и мсбласта стало ясно, что фаервол необходим. Более того необходим двухсторонний фаервол , который бы смотрел исходящий трафик, чтобы отлавливать действия Троянов претворяющихся нормальными приложениями. Именно этими фактами вызвано встраивание IDS компоненты в рабочие станции Касперского, создание Симантеком Client Security, встраивание в Нортон фичи Internet Worm Protection – по сути одностороннего фаервола и наконец выпуск KIS6.0.

Оставаться чистым антивирусом здорово, но ваши пользователи либо по незнанию будут оставаться без должной защиты, либо будут пользоваться набором решений от разных производитлей – что, во-первых, не всегда удобно, во-вторых, может приводить к конфликтам программ, в – третьих, не позволяет обеспечивать взаимодействие между различными компонентами защиты. А для корпоративных пользователей встает еще и проблема администрирования всего этого зоопарка.

Вы же включаете в свои продукты сигнатуры шпионских программ, зачем? Это ведь не антивирус, это совсем другой продукт!!!!

А еще странно слышать такие заявления при условии, что у вас на сайте проводился опрос нужен ли фаервол и домашние пользователи сказали – да нужен. И вы по слухам это фаервол даже разрабатываете. Тогда зачем такие заявления?

Говорят, что антивирус Dr.Web - ресурсоемкая программа

Ну это реально миф, наверное это вы чтобы себя похвалить включили☺

Кроме того, в программе есть специальные настройки, которые позволяют еще больше экономить ресурсы компьютера - но уже за счет безопасности пользователя. Любой выигрыш в скорости и ресурсоемкости обычно дается за счет снижения уровня безопасности. Огромное преимущество Dr.Web перед другими аналогичными программами - возможность весьма тонкой настройки.

Вот видите у вас тоже есть специальные настройки, которые позволяют экономить ресурсы в ущерб безопасности. А говорили порочная практика, А я яй

Ходит миф, что Антивирус Dr.Web не поддерживает Windows 98, Me, NT 4.0

Ну это реально миф, наверное это вы чтобы себя похвалить включили☺

Ходит миф, что в антивирусе Dr.Web нет возможности проверки архивов "на лету" до записи на жесткий диск.

ДА это реальный миф

Ходит миф, что в антивирусе Dr.Web нет возможности восстановления системы после вредоносного воздействия.

Если речь идет о ситуациях, когда системные файлы безвозвратно испорчены вирусом, то в Dr.Web такой возможности действительно нет. Но это и не функция антивируса. Есть специализированные программы, занимающихся резервным копированием критических данных пользователя, а также стандартные средства восстановления системы, встроенные в Windows. Ряд антивирусных производителей говорят о том, что в их продуктах есть возможность восстановления системы, однако что они под этим имеют ввиду, известно только им одним.

Замечание сверх странное. Речь идет о том, что вредоносный процесс производит изменения в системных и других файлах, а также реестре. Если это известный вирус, то может быть предусмотрено лечение – т.е. откат изменений (а поскольку вредонос известный, то и изменения, который он делает тоже известны). Так делает трендмайкро например или утилита долечивании Касперского. Если вредонос неизвестный, то как только какой-то процесс начинает себя подозрительно вести, можно начать фиксировать все изменения, которые он производит в системе, а потом если процесс признается вредоносным эти изменения откатывать – так делает Касперский в своей проактивке.

Мифы о почтовом мониторе SpIDer Mail

Ходит миф, что антивирус Dr.Web не может проверять сообщения, поступающие по протоколу IMAP "на лету", причем независимо от того, какой тип почтового клиента используется.

Это миф. 11.05.2006 вышла обновленная версия SpIDer Mail, в которой данная возможность присутствует, независимо от типа почтового клиента, причем на сегодняшний день только антивирус Dr.Web максимально корректно обрабатывает почту, поступающую по протоколам IMAP\NNTP.

Что не лечит – это реально миф. НО ваши заявления про уникальность: “Компания «Доктор Веб» - ведущий российский разработчик и поставщик средств антивирусной безопасности - уже сообщала (новость от 11 мая 2006 г.) о выпуске уникальной технологии антивирусной проверки электронной почты, получаемой по протоколу IMAP, а также новостных сообщений, получаемых по протоколу NNTP.” Это реальный миф IMAP на лету лечит 6.0 Касперского, NNTP уже давно Панда, недавно Касперский.

Ходит миф, что в антивирусе Dr.Web не существует возможность задания порта в настройках для проверки почтового трафика

Да это миф.

Мифы о вирусных базах Dr.Web и об их обновлениях

Говорят, что у антивируса Dr.Web крайне редкие обновления - раз в неделю

Да это миф. За последний год у Доктора с этим делом грандиозное улучшение. Но во-первых, у того же Касперского обновления выходят чаще. Например (это из документов вендоров) за 2005 годДоктор Веб - 5751 обновлений, что составляет в среднем 15,7 раз в сутки ЛК -7021, 19,2 в сутки
Кроме того взгляните внимательно сюда: http://updates.drweb.com/
Если внимательно изучить эту статистику, то видно что Доктор Веб выпускает очень интересно:

```
dwntoday.vdb (2006-05-25 13:18:04, MD5: 4fb8fcf8983a56d349914482996943b5)
drwtoday.vdb (2006-05-25 13:18:14, MD5: cbecc9300d1f6236aeffa7184e14244b)

dwrtoday.vdb (2006-05-25 14:13:20, MD5: befdb8bb70f33a53db97981e929a2183)
dwntoday.vdb (2006-05-25 14:13:30, MD5: 453e48ea339fa289ad8b5912bf32ac73)
```

Прикольно правда? Обновления выходят с разницей в несколько секунд, и такая история каждый день. То есть ребята просто делят обновления на несколько частей, выпускают их с разницей в несколько секунд в итоге статистика растет со страшной силой. Здорово.

Ходит миф, что антивирусная база Dr.Web самая компактная потому, что "знает" мало вирусов.

Да это не совсем правда Доктор Веб действительно много времени уделяет оптимизации базы. Но согласно тесту http://www.av-comparatives.org/seiten/ergebnisse_2006_02.php уровент детекта у доктора веба 88,76%, а это значит что пропустили в ходе теста они около 18000 вредоносов (это без ДОС вирусво).

Ходит миф, что антивирусная база Dr.Web самая компактная потому, что старые вирусы просто выбрасываются из базы данных сигнатур. Поэтому антивирусная база Dr.Web компактна и проверка проходит быстро.

Это неправда. Никакие вирусы из базы не выбрасываются. Подтверждение тому - успешное участие Dr.Web в тестировании антивирусов редакцией журнала Virus Bulletin. В предлагаемых на этих тестированиях коллекциях есть вирусы практически всех поколений.

Ну да, наверное не выбрасываются, но тетст VB100%, который проводится на максимум 5000-6000 вирусах (это сейчас, а раньше еще меньше) – это вряд ли объективный показатель. Как я уже говорил выше VB100% - это обязательный минимум, который надо выполнять, но вовсе не объективный показатель эффективности.

Ходит миф, что в Антивирусе Dr.Web нет возможности обновления баз продукта по расписанию

Это миф. В Dr.Web есть собственный Планировщик. Он устанавливается по умолчанию, и в нём есть задание, настроенное по умолчанию на получение баз один раз в час. Это не мешает настроить получение обновлений вирусных баз на несколько раз в течение часа. В последнее время это довольно часто имеет смысл.

О да это прекрасно, но задать время обновления – например 12 часов ночи в Dr.Web насколько мне известно – нельзя.