Прививка от вирусов
Выбираем отечественные средства?

По просьбе читателей редакция «Системного администратора» организовала с компанией «Доктор Веб» заочный круглый стол по проблемам выбора и применения антивирусного ПО. Какие антивирусные программы предпочитают пользователи? И чьего производства — зарубежного или российского? На вопросы отвечает ведущий аналитик отдела развития компании Вячеслав Медведев

Развенчание мифов

– Существует мнение, что время антивирусов уходит в прошлое, а на смену им приходят новые, более эффективные средства защиты. Согласны ли вы с этим?
– Нет. Я за время своей работы в отрасли слышал это не раз. Об активных технологиях, облачных антивирусах... Времена меняются, но замены антивирусу быть не может. Обнаружить и пролечить активную инфекцию может только он.

– Я давно отказался от семейства Windows в пользу Ubuntu. За свою практику разработки за последние пять лет, с тех пор как пересел на Ubuntu, я не имел ни одного случая вирусного заражения. Хотя, нет, лукавлю: три-четыре года назад подцепил известный вирус на Mac OS, который замаскировался под Adobe Flash Player. Не надо совать свой нос туда, где есть рассадник инфекции.
– Опасное заблуждение. Что есть рассадник инфекции? Сайты с порнографией? Отнюдь. Они заинтересованы, чтобы их посещали, и заботятся о своей репутации – тем более что на них и так вешают все грехи вирусов. А вот на новостные, финансовые и прочие сайты внимания не обращают. На них ходят все, но почему мы должны им доверять? Статистика http://www.ptsecurity.ru/download/PT_Web_application_vulnerability_2014_rus.pdf страшна.

2014-й стал годом резкого роста интереса к Mac и Linux. Я думаю, о количестве найденных уязвимостей в Linux слышали все. Такого их урожая еще не было – и это только начало. Соответственно выросло и количество вирусов – если ранее в год для них находилось менее десятка угроз, то в этом году ситуация совсем иная. И мифы о неуязвимости работают на хакеров.

P.S. В час, когда писался ответ, на Украине пользователи утилиты CureIt! нашли 2386 вредоносных программ – и это только то, что пропустили иные системы защиты.

P.P.S. В России за этот же период было поймано «за руку» еще 12 502 вредоносные программы.

– Всегда ли нужен любой антивирус?
– Всегда. И не любой.

Новая версия – новые возможности

– В этом году вышла десятая версия вашего продукта – какие новые возможности она предлагает?
– В этом году вышло две десятых версии – сначала корпоративная (Dr.Web Enterprise Security Suite), а затем и версия для домашних пользователей (Антивирус Dr.Web и Dr.Web Security Space). Обновились версии для мобильных устройств (хитом стала версия с технологией «вытряхивания» блокировщиков), в ответ на рост новых угроз чуть не вдвое вырос функционал решений для Mac и Linux…

Если говорить о Dr.Web Enterprise Suite, то документ со списком изменений потянул на десяток листов – с кратким обзором нововведений вы можете ознакомиться в статье http://samag.ru/archive/article/2771.

– Не очень удобен переход со старой версии на новую – использование инструкции не гарантирует 100% успешной установки. Проводят ли ваши эксперты тестирование переустановки, и что проверяется в ходе такого тестирования?

О компании

Российская компания «Доктор Веб» разрабатывает антивирусные продукты, востребованные как частными пользователями, так и бизнесом, а также госструктурами. Оперативно отвечая на «вирусные вызовы» сегодняшнего дня, разработчики внедряют в продукты Dr.Web самые современные технологии, позволяющие противостоять актуальным опасностям, в том числе «энкодерам» и банковским троянцам. Под надежной защитой Dr.Web сегодня находятся не только миллионы компьютеров, но и мобильные устройства по всему миру (Dr.Web для Android стал одним из популярнейших средств для защиты этой платформы, он скачан с Google play более 70 000 000 раз). Недавно увидела свет 10-я версия Dr.Web – и для корпоративных, и для частных пользователей: уровень защиты Dr.Web от современных вредоносных объектов был повышен, а управление настройками максимально упрощено. При этом непрерывно идет работа над дальнейшим совершенствованием продуктовой линейки Dr.Web.

– Тестирование проводится. Причем не только сотрудниками отдела тестирования. Мы стараемся привлечь максимальное количество участников для этого и выявить проблемы до релиза. В частности, я также тестировал наш новый продукт – в том числе и процесс обновления. К сожалению, наш антивирус работает в самом разном окружении, с самыми разными настройками. Поэтому после релиза мы направили максимальные усилия на то, чтобы выявленные пользователями проблемы устранялись максимально оперативно.

– Как относятся в компании к предложениям пользователей о том, что нужно что-то улучшить в продукте? Учитывают ли их при доработке решений? Как долго длится эта доработка?

– Естественно, мы стараемся принимать во внимание пожелания, но, к сожалению, учесть все невозможно. Только мой список с кратким описанием пожеланий для Dr.Web для Windows сейчас превышает 23 страницы.

Естественно, пользователи хотят получать нужный им функционал. Но не все желаемое – безопасно. Достаточно много решений имеет изъяны, о которых умалчивают те, кто пропагандирует «революционные» технологии. И, получив такой функционал, пользователь может оказаться менее защищен, чем до этого, ведь пропагандисты революции о проблемах умолчали. Компания «Доктор Веб» выпускает только то, в чем уверена, – уязвимостей быть не должно.

Главный функционал антивируса скрыт от пользователя. Технологии обнаружения и лечения работают незаметно (хотя те, у кого сканер создал нагрузку, с этим поспорят). Появление все новых и новых инфекций требует постоянного отвлечения ресурсов на совершенствование (тестирование, документирование…) этих бойцов невидимого фронта.

Практическая безопасность

– Может ли Dr.Web обнаруживать и предотвращать заражение ПК, файлов от шифровальщиков вроде key.privet?

– Коллективный разум так и не смог определить, что есть key.privet, поэтому немного теории. Нас постоянно спрашивают, ловим ли мы те или иные вирусы. СМИ рекомендуют ставить, кроме антивирусов, еще и антиспуваре и антируткиты. Так вот. Вредоносная программа – это программа, которая ставится без уведомления пользователей и выполняет действия, о которых пользователь не был предупрежден при установке. Поэтому никаких «антиххх», кроме антивируса, не нужно.

Теперь об «обнаруживать и предотвращать». Любой антивирус может поймать только ту программу, алгоритм действия или сигнатура которой ему известны. Это касается и сигнатур, и эвристики, и поведенческого анализатора. Естественно, есть технологии, направленные на обнаружение новых вредоносных программ, еще не попавших к нам на анализ, но нужно понимать, что злоумышленники тестируют свои «произведения» на актуальных версиях антивирусов, и поэтому предотвращать заражение нужно не только с помощью антивируса. Может возникнуть мысль, что от антивируса в этих условиях толку нет. Да, снизить риск проникновения можно и без антивируса. Но только антивирус может обнаружить ранее неизвестную угрозу, обошедшую все рубежи защиты, и пролечить систему.

Кстати

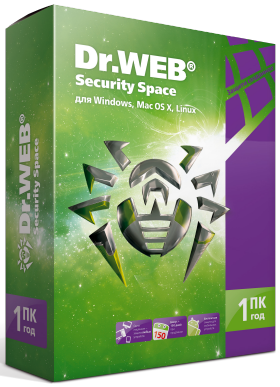
Согласно опросу, проведенному редакцией среди читателей журнала «Системный администратор», антивирусное ПО компании «Доктор Веб» входит в тройку лидеров по частоте использования. При этом в организациях и компаниях респондентов антивирус Dr.Web на втором месте, а что касается домашних пользователей, то среди них – на третьем.

И о «пролечить». Антивирус может обнаружить и удалить любую вредоносную программу известного типа, но вот откатить результаты ее деятельности он не в силах. Естественно, современные антивирусы (и Dr.Web в их числе) имеют функцию резервного копирования, но нужно понимать, что встроенные в антивирусы средства резервирования уступают специальным решениям для бэкапа.

– Многие пользователи, особенно неопытные, сталкиваются с атаками злонамеренного ПО. Чтобы избежать этого, приходится шифровать документы и файлы на своем компьютере. Стоит ли ждать от «Доктора Веб» эффективного решения данной проблемы?

– Один в поле не воин. Как уже говорилось, мы можем ловить и удалять любые известные типы вредоносных программ, но решить проблему беспечности наших клиентов мы не в состоянии. Скажем, для предотвращения заражения неизвестными шифровальщиками и блокировщиками у нас есть поведенческий анализатор. Но он запускается после старта программы, и до того момента, когда он выдаст свой вердикт, несколько файлов уже могут пострадать. Да, мы можем расшифровать результаты деятельности троянца (и есть случаи, когда за расшифровку не брались даже наши конкуренты). Но надо понимать, что против нас работают профессионалы – расшифровка возможна не всегда. Поэтому резервирование и система ограничения доступа – «минимум миниморум» безопасности. И о внимательности к открываемым письмам. Да, случаи заражения через письма (как и через флешки) были, есть и будут. Но практика показывает, что крайне мало специалистов знают об основном пути заражения. Свыше 80% сайтов имеет уязвимости (по статистике Positive Technologies), большинство людей посещают одни и те же интернет-ресурсы, работают с необновленными версиями программ. Зачем ломать компании поодиночке, когда можно взломать один сайт, и жертвы сами туда придут?

– Какой документацией можно пользоваться при развертывании Enterprise Security? Решение интересное, хотелось бы изучить подробно.



– Естественно, есть полная документация по продукту. Кроме этого, имеется учебный курс – документ, созданный в виде пошаговых инструкций для наиболее востребованного функционала. Необходимо также сказать, что протестировать наши продукты можно с помощью сервиса Dr.Web LiveDemo. Разместить заявку на предоставление доступа к виртуальным машинам можно по адресу: https://

download.drweb.com/live_demo/?lng=ru. Кстати, в журнале «Системный администратор» не так давно была статья от одного из разработчиков этого сервиса о том, как все реализовано, и какие подводные камни встретились по дороге.

– Почему упало качество антивирусного решения в последних версиях?

– Упало не качество антивирусов – созрел рынок вирусных «изделий». Давайте так. Сколько вредоносных файлов приходит нам на анализ? Загадываем цифру, а затем идем на http://live.drweb.com, закладка Infected Objects. И это далеко не все, что создано в этот день. Раньше вирусы создавали для того, чтобы прославиться, и иногда даже прямо присылали (и приходили) в антивирусную компанию, чтобы их просто добавили в базы. Теперь это рынок. На нем можно купить троянца, нанять дропперов, обналичить деньги. Вредоносные программы разрабатываются на потоке. До 100 образцов в день от одной только группи-

Антивирусу необходимо знание о максимальном количестве угроз. И тут отечественные решения вне конкуренции — количество записей в вирусных базах говорит само за себя

ровки, и ни один не ловится ни одним антивирусом. Почему так грустно? В таких группах есть исследователи, разработчики, партнерская программа и борьба с нелицензионным использованием. Но самое главное – тестировщики, о которых мы уже говорили. Естественно, мы стараемся этому противодействовать. В числе наших технологий – ScriptHeuristic (предотвращает исполнение любых вредоносных скриптов в браузере и PDF-документах, защищает компьютер от заражения неизвестными вирусами через веб-браузер), технология несигнатурного поиска Origins Tracing (позволяет с высокой долей вероятности распознавать вредоносные программы, еще не внесенные в вирусную базу), FLY-CODE (технология универсальной распаковки файлов, запакованных неизвестными упаковщиками)...

– В чем состоят новшества в процессе реализации решений безопасности для Windows 10 в отличие от предыдущих версий?

– С точки зрения разработки единственным принципиальным отличием Windows 10 от Windows 8.1 является новая подсистема блокировки устройств DeviceGuard, позволяющая осуществлять блокировку шин, классов устройств, вести «белые списки».

– У компании «Доктор Веб» есть интересное предложение – «антивирус как услуга». Насколько востребовано оно сегодня? Для каких компаний (по численности персонала) эта услуга предназначена?

– В настоящее время сервис Dr.Web AV-Desk предоставляют более 350 партнеров из многих стран мира – прежде всего это операторы связи, банки, ИТ-аутсорсинговые компании, а общее количество подписчиков перевалило за 1,3 млн. Если говорить о защите бизнес-пользователей, то сервис Dr.Web AV-Desk может использоваться для защиты компаний, относящихся к СМБ, с любым количеством защищаемых объектов. Решение для бизнеса позволяет клиентам, в том числе не имеющим постоянных системных администраторов, получать защиту Enterprise-класса с централизованным управлением компонентами для рабочих станций (MS Windows/MAC OS), файловых серверов (Windows Server) и мобильных устройств под управлением Android. Использование сервиса (в том числе за счет помесячной оплаты услуг сервиса) позволяет на 70-80% снизить совокупную стоимость владения антивирусом по сравнению с классическими решениями.

Импортозамещение и все-все-все

– Антивирусы: надежно ли защищают они сегодня ПК и мобильные устройства от всевозможных угроз? Насколько с этим справляются отечественные антивирусы?

– Чуть выше говорилось о том, как разрабатываются сейчас вредоносные программы и почему их пропускают антивирусы. Не будем повторяться. Ни один антивирус из тех, на которых вирусописателями ранее тестировалась новая, не поступившая еще на анализ в вирусные лаборатории инфекция, не сможет предотвратить ее проникновение (часто даже средствами эвристики (вообще, всемогущество эвристики – это тоже распространенный миф) или иных технологий) до получения пользователем обновления, в котором уже внесена информация о ней. Задача антивируса – не только и не столько пытаться помешать проникновению – это можно сделать и иными методами. Основная цель антивируса, задача, которую, кроме него, не может выполнить никто, – лечение ранее пропущенных инфекций, уже запущенных и активно противодействующих своему обнаружению и удалению.

Антивирус должен иметь эффективную самозащиту (ничто не должно нарушить его работу) и отличную систему лечения активных заражений. Как ни странно, как правило, при выборе средств защиты именно эти два параметра игнорируются чаще всего, а ведь именно они – фишка отечественных решений. Обязательны наличие системы сбора образцов новых вирусов на той территории, где работают его пользователи, постоянный выпуск новых технологий, направленных на поиск, обнаружение и уничтожение вредоносных файлов.

Необходимо знание о максимальном количестве существующих угроз. И тут отечественные решения вне конкуренции – количество записей в вирусных базах говорит само за себя. Требуется максимально быстрое и частое обновление баз. По статистике «Сбербанка», время вывода денег со счета составляет от одной до трех минут. Антивирус должен обновиться быстрее! Ну и документация на русском языке и местная, находящаяся в России, техподдержка – желательно без разделения на первую и вторую линию.

Кроме антивируса, в систему защиты должны в обязательном порядке входить система ограничения прав доступа и запуска программ (ничто неизвестное не должно запускаться) и система резервирования.

Ну и не все зависит от производителя – зачастую на момент заражения в базах уже есть информация об угрозе, но пользователи не обновляются, не любят перезагрузки.

– Многие корпоративные пользователи покупают антивирусы сразу нескольких компаний-производителей, чтобы не быть привязанными к одной технологии...

– Есть стандарты и документы регуляторов (например, СТО БР РФ), рекомендующие делать именно так. И, как правило, несколько антивирусов используется в компаниях, находящихся в зоне действия таких стандартов/рекомендаций.

– Есть ли какие-либо сигналы с рынка, свидетельствующие о том, что компании и пользователи в России стали отдавать предпочтение отечественным антивирусам?

– В среде крупных компаний однозначно лидируют отечественные решения, доля зарубежного ПО крайне мала. Для малого и среднего бизнеса тенденция перехода на отечественные антивирусы также заметна.

– Готовится ли компания «Доктор Веб» к приему закона о запрете использования импортного софта при наличии двух российских аналогов?

– Нам готовиться не нужно: мы чисто российская компания.

– Считаете ли вы этот закон правильным?

– Частично. Огульно запрещать не стоит, конечно, но проектировать системы безопасности госкомпаний и критически важных объектов с учетом возможных проблем, естественно, нужно. Террористов, хулиганов, да и просто коммерческую разведку никто не отменит. Я бы приветствовал движение в сторону поддержки разработки отечественного ПО.

– У нас в компании стоит антивирус Касперского. А дома у меня вообще никакого нет. Винда у меня насмерть заэкранирована, а от вирусов на флешках спасает линуксовый образ «Доктор Веб». Почему вообще люди продолжают покупать импортный софт? Привычка? Техническая инерция, нежелание изучать новое?

– Я бы добавил: практическое исчезновение правильных сравнительных тестов программ. Их заместили обзоры на тему, как хорошо ставится продукт.

– Долгое время я был приверженцем отечественного продукта – Dr.Web. Но последние релизы вызывали лишь негативные эмоции. Не проще ли выбрать альтернативное решение? Я не делаю ставку на отечественный или зарубежный продукт. Мой главный критерий выбора – качество.

– Качество – это, естественно, правильный выбор! Но каковы его критерии? Количество пропущенных вирусов? Скорость работы? Зачем вам нужен антивирус? Вы твердо уверены в этом? Антивирус – единственное средство, умеющее лечить ранее неизвестное, и тут, как мы считаем и как показывают имеющиеся тесты, отечественному соперников нет. Если говорить о нас, то фишкой именно нашего антивируса является развитие средств обнаружения и лечения активных угроз, ввод в строй новых «ядерных» технологий.

Будущее – ближайшее настоящее

– Планирует ли ваша компания предпринять какие-то меры, чтобы в 2015 году укрепить свои позиции в сфере домашних антивирусов?

– Будем стремиться как можно более незаметно и неотвратимо находить и обезвреживать. Пишется новое ядро, прорабатываются новые технологии. Планов очень много.

В нашем бизнесе трудно загадывать на будущее. Иногда проделанная работа в момент перечеркивается выходом обновлений операционной системы или появлением нового типа вируса.

– Наша компания перешла с антивируса Symantec на Dr.Web. К сожалению, центр управления у Dr.Web не так удобен по сравнению с Symantec. Можно ли улучшить дизайн и сделать более удобным управление?

– Мы думаем над этим. К сожалению, смена интерфейса – не только трудоемкий процесс, но и психологическая проблема. По статистике, одна из трех основных причин смены антивируса – изменение его интерфейса. В десятой версии мы существенно переработали систему оповещений, расширили статистику… В следующем году будет новая версия – и в ней уже запланировано много нововведений, как мы надеемся, приятных для администраторов и пользователей.

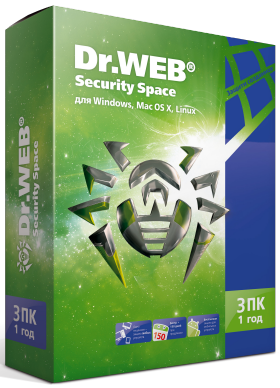
– Каким видится будущее операционной системы Android в плане обеспечения безопасности? Можно ли ожидать роста угроз? Можно ли говорить о повышении безопасности Android с выходом версии 5?

– Ожидать роста угроз не нужно. Он уже есть. Год еще не кончился, поэтому цифр роста за этот период еще нет. Итоги 2013 года можно посмотреть в новости http://news.drweb.com/show/?c=5&i=4211&lng=ru. За 2014 год рынок вредоносных программ «дозрел». Появились локеры, новые банковские троянцы (http://news.drweb.com/show/?c=5&i=7091&lng=ru)... Преступники стали использовать для распространения списки контактов жертв и СМС (http://news.drweb.com/show/?c=5&i=7076&lng=ru), встраивать троянцев в образы альтернативных прошивок (http://news.drweb.com/show/?c=5&i=7071&lng=ru)...

Проблема Android – в огромном числе необновляемых версий прошивок и моделей телефонов. Версия 5, естественно, имеет новые средства обеспечения безопасности – но вспомним, сколько раз производители иных ОС говорили нам, что уж в этой версии ОС ни одного вируса не будет! Количество вредоносных программ – это мера популярности системы.

– Что можно сказать о будущем в плане безопасности ОС Linux с учетом, например, обнаружения уязвимости Shellshock?

– Ничего нового, кроме того, о чем давно предупреждали специалисты по безопасности. Linux не настолько отличается от иных ОС, чтобы не иметь уязвимостей. И можно сказать, что хакеры только начали работу над исходниками. Мне приятно отметить, что наша компания первой отреагировала на данную тенденцию, добавив модули проверки трафика в наши решения для Linux и Mac.



– Можно ли рассчитывать на изменение в продукте «Доктора Веб» концепции антивирусной защиты виртуальной среды без установки на каждую виртуальную машину агента, подобно deepsecurity?

– Лично я надеюсь, что мы не будем выпускать такой продукт, так как он не обещает возможности решения проблем с защитой. Интересующихся отсылаю к известной статье Евгения Касперского «Амбиции, лень и жадность в IT-бизнесе».

К сожалению, пиар-технологии зачастую вызывают к жизни редкостные вещи. СМИ рекомендуют, заказчики требуют, маркетологи считают прибыль, злоумышленники с удовольствием используют. Не нужно читать газету «Правда», описывающую прелести будущего с новыми технологиями. По дороге до него кормить не будут.

Предотвратить проникновение (точнее, снизить риск) можно и без антивируса. Но только антивирус может обнаружить ранее неизвестную угрозу, обошедшую все рубежи защиты, и пролечить систему

– Почему компания «Доктор Веб» уделяет мало внимания рекламе своих продуктов? А ведь антивирус Dr.Web – единственный по-настоящему российский антивирус (та же «Лаборатория Касперского» частично принадлежит американцам – 20% акций). Именно в антивирусах «Доктора Веб» появлялись передовые технологии борьбы с вирусам!

– Во-первых, «Лаборатория Касперского» давно уже выкупила те свои акции, ну а насчет роста и маркетинговых усилий: «Рост рынка антивирусов в России в 2013 году – 9,2%» (Источник: IDC). Рост активаций серийных номеров на Dr.Web Security Space: январь – октябрь 2014 года, электронные лицензии, 1-5 ПК – 58%. Как вы думаете, можно ли объяснить этот рост «агрессивной рекламой некоторых антивирусных продуктов и прочими маркетинговыми ходами производителей антивирусного ПО»?

И спасибо за высокую оценку наших технологий!

О бедном гусаре замолвите слово

– Многие антивирусы для домашнего пользователя предлагают свое ПО бесплатно (базовый набор). Почему для ПК компания «Доктор Веб» по-прежнему использует старую схему, а для Android такое ПО бесплатное?

– В свое время один очень известный человек сказал: «Наш антивирус будет бесплатным, когда в России не будет налогов на автодороги». Разработка стоит дорого (и мы молчим о налогах). Сравните количество продуктов, частоту обновлений, степень локализации и уровень техподдержки у бесплатных и коммерческих решений.

Касаясь Android. Во-первых, полная версия – с антиспамом, антивором и прочим – платная. Бесплатна только версия Light. Почему так? На то есть исторические причины. Первые антивирусы для Android появились в момент, когда угрозы для этой ОС были по большей части мифом. Нас просили об антивирусе – и мы его реализовали. Но брать деньги за защиту от того, чего нет, не стали. С тех пор прошло много времени. Вирусы для Android давно уже не редкость, но мы не хотим лишать защиты тех, кто верен нашим решениям.

– Почему бы не вернуться к бесплатным лицензиям на антивирусное ПО «Доктор Веб» для образовательных учреждений? Также можно организовать бесплатные лицензии для студентов. Ведь выгода компании все равно от этого будет. Попробовав, студенты и дальше будут использовать ваши антивирусы. Почему до сих пор нет бесплатной корпоративной версии? Будет ли она в ближайшее время? При ее наличии популярность продукта выросла бы в разы.

– Мы уже говорили о бесплатной раздаче продуктов исходя из стоимости разработки и поддержки. Посмотрим с другой стороны: а увеличит ли количество пользователей и прибыль (будем реалистами – любая компания работает за деньги) бесплатная версия? Поговорим о студентах и их влиянии на использование ПО. Часть студентов считает себя крутыми хакерами, часть – крутыми админами, которые настроят свою систему так, что ничто вредоносное не проползет. Администрация зачастую отказывается защищать кампусы по причине того, что бестолку. Будут ли защищены студенты, поставив бесплатную версию? Уже упоминавшаяся статистика CureIt! показывает, что происходит с теми, кто не знает основ безопасности и целиком полагается на бесплатное. Кто будет в этом виноват? Но, предположим, студент стал фанатом отечественного ПО и пришел на работу. Он будет использовать только российское? Увы и ах. ПО закупается решением руководства компании, а зачастую еще и руководством не того филиала, в котором работает сотрудник, а организации в целом. Большая компания – лакомый кусочек, и с ее руководством ведут умелые переговоры – есть ли в них место недавнему студенту? И, кстати, вопрос: почему бы врачам не ввести практику бесплатного оказания услуг – с бесплатной же доставкой больных, выдачей им необходимых лекарств и приборов для лечения? Ведь это увеличит как узнаваемость врачей, так и количество их клиентов!

– Почему «Доктор Веб» не выпускает бесплатную версию антивируса для пользователей? На Windows 7 я пользуюсь, например, антивирусом от Microsoft. Это не самое лучшее решение, но по крайней мере оно бесплатное, его можно скачать без регистраций и смс.

– Не буду заниматься антирекламой конкретных продуктов, но крайне рекомендую посмотреть на тесты лечения активных заражений (а это единственные тесты, кроме тестов на самозащиту, которые заслуживают внимания) и изучить, какие места в них занимают бесплатные решения.

– Я бы с удовольствием переключился на тот же Dr.Web, если бы он был бесплатный, пусть и с минимальным функционалом, но именно бесплатный, чтобы обойтись без вбивания секретных кодов, активаций и других трюков, а уж если кто хочет какой-то особый функционал, пусть покупает лицензии.

– Что есть ненужный функционал? Пройдемся по персональной версии, например. Dr.Web Security Space состоит из:

системы проверки почтового и интернет-трафика. В отличие от ряда иных решений проверяет трафик до получения его клиентскими приложениями (исключение – протокол MAPI, но тут деваться некуда, так как он закрытый). Соответственно снижает риск использования неизвестных пока уязвимостей этих приложений вредоносными программами/злоумышленниками;

файлового монитора. Проверяет все запускаемые программы на известные инфекции. Тут, наверное, понятно;

системы проверки процессов – обеспечивает обнаружение ранее неизвестных вредоносных программ (о которых антивирусу стало известно после обновления);

поведенческого анализатора – обеспечивает обнаружение вредоносных программ, еще не поступивших на анализ в нашу лабораторию, но имеющих известно-опасное поведение. Как бы тоже нужная вещь;

системы ограничения доступа. Блокирует доступ к потенциально опасным ресурсам – в том числе если обращение исходит не только от самого пользователя. Вы уверены, что неизвестная программа не обращается куда-либо?

системы самозащиты. Не позволяет неизвестным пока нам инфекциям нарушить работу антивируса;

системы лечения активных инфекций. Тоже нужно.

Это, конечно, крупными мазками, аналогично можно разобрать и на более глубоком уровне. Наши решения не включают ничего, кроме необходимого для защиты, – это отличительная черта наших продуктов.

Если в Dr.Web есть функционал, который не нужен, укажите на него нам, и мы его уберем. А еще лучше – предлагайте свои технологии, позволяющие уменьшить «прожорливость» систем защиты, и приходите к нам.

– На устройствах с Windows 8.1 и Windows 7 у меня только антивирус Avast. Почему? Если говорить о Касперском или Dr.Web, то есть множество напрягающих факторов по сравнению с Avast. Что-то надо регистрировать, что-то с ограниченным функционалом, в то время как Avast просто предлагает бесплатный функционал в течение года. Платить за защиту от неочевидных вирусов не хочется. Читать обозрения о них же тоже неинтересно. Зачем мне об этом знать в подробностях? Я же не вирусописатель...

– Пожалуй, переставлю два предложения местами. «Читать обозрения о неочевидных вирусах неинтересно. Платить за защиту от них же тоже не хочется».

Практика общения с клиентами и участие в конференциях показывает, к чему эта позиция приводит – 19 из 20 компаний не знают, как на самом деле проникают вирусы в их систему, зачем им нужен антивирус и как защищаться от вредоносных программ. Почему-то считается, что, поставив любой антивирус из числа победителей в тестах, можно проблему с вирусами решить автоматически. Ну, еще, конечно, включить до упора все опции проверки. К сожалению, аналогичная логика прослеживается в приказах регуляторов. В результате, формально выполнив требования приказов по антивирусной защите, компании и пользователи остаются беззащитными. И первый же пропуск троянца становится шоком и поводом к смене продукта, но не к совершенствованию системы защиты. Информации о том, как защищаться, – вагон, но «читать… неинтересно». Страшная тенденция – все ходят на конференции и ждут, что им все расскажут и разжуют. Мне ежедневно поступают запросы на тему, какие у нас системные требования, – открыть сайт и прочитать уже стало сложно.

– На аппарате Samsung Galaxy 2 (платформа Android) я долгое время использовал Dr. Web. Что заметил? Большое время загрузки, достаточно частые сбои: «Не смог загрузиться», «Не смог прочитать карту памяти» и т.д. Поэтому на новый Galaxy S5 уже не стал его ставить.

– Просьба сообщить номер запроса в техническую поддержку. Поймите, мы не волшебники (хотя и стараемся). Чем больше нам сообщать о проблемах – тем лучше станет продукт. BOF