Dr.Web Security Space 10: российская защита

Игорь Новиков

На рынке антивирусов сегодня наблюдаются как минимум две тенденции: постепенный отказ от сигнатурных методов в качестве базовой защиты и усиление внимания к нормативной базе, на соответствие которой проверяются устанавливаемые программы.

Первый тренд коренным образом поменял алгоритмы, на которых построены современные антивирусные средства. Вместо прежнего запрета запуска программ по «черным» спискам вирусов наблюдается переход к использованию «белых» списков при построении

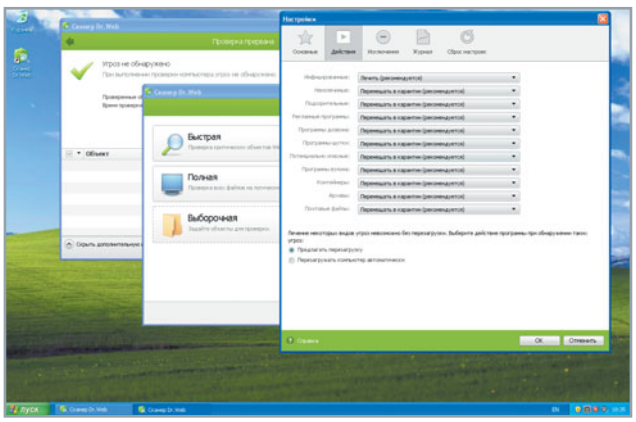
программной среды. Система выстраивается так, чтобы в ней мог работать только проверенный программный код, в который не вносятся никакие изменения после прохождения этапа проверки.

Второй тренд повысил значимость нормативной базы. Наблюдается отход от концепции «тотальной защиты» компьютеров и переход к управлению рисками и гарантией соответствия требованиям различных нормативных документов, например, PCI DSS.

Причина таких изменений состоит в том, что прежняя концепция организации антивирусной защиты была основана на реалиях 20-летней давности. Тогда каждый отдельно взятый компьютер рассматривался как «крепость», которую надлежало сделать неприступной. Сегодня пришло время устройств BYOD, когда даже дома в распоряжении пользователя есть как минимум три—четыре устройства, которые могут быть атакованы вирусами. Ситуация усложняется еще тем, что устройства работают на разных ОС.

Хороший вирус — пойманный вирус!

Поэтому смысл прежней защиты, выстраиваемой вокруг отдельного компьютера, потерял актуальность. Компрометация данных может произойти в любом месте. Прежние антивирусные системы работают, но теперь их нужно дополнять новыми инструментами.



Развитие популярного российского антивирусного продукта Dr.Web шло в русле наметившихся перемен. Создавая новую версию Dr.Web Security Space 10, разработчики продолжили развивать единую платформу защиты. Сегодня это комплекс средств: «Антивирус», «Антишпион», «Антируткит», «Антиспам», «Веб-антивирус» и «Родительский контроль». Установка ключевого файла программы позволяет бесплатно пользоваться программой Dr.Web Mobile Security Suite, которая создает заслон от проникновения вредоносного кода со стороны мобильных устройств.

Алгоритмы защиты современных версий Dr.Web основаны в первую очередь на выявлении вирусных действий на компьютере, а не только на обычном сравнении сигнатур с уже выявленными вирусами. Прежний подход стал затратным с точки зрения использования системных ресурсов, да и опираться на сигнатуры бесполезно, когда речь идет о новых угрозах, которые распространяются в течение одного—двух дней.

Алгоритмическая защита позволяет при небольшом числе записей в базе сигнатур надежно детектировать вирусы и вредоносные программы. Такой метод не только экономит место на диске, сохраняет ресурсы оперативной памяти, снижает трафик при обновлении баз, но и позволяет с высокой скоростью анализировать программы на вирусы и определять модификации уже существующих версий. Обоснованность выбора ясна: число реально встречающихся алгоритмов построения вирусов не так уж велико, и основная их часть — это не оригиналы сигнатур, а их модификации.

Принцип «умной» защиты новой системы Dr.Web состоит в обнаружении и обезвреживании неизвестного вредоносного ПО с использованием несигнатурных технологий. С помощью подсистемы *Fly-Code* выполняется проверка упакованных исполняемых объектов. Она способна распаковывать файлы, обработанные любыми, даже нестандартными, упаковщиками, благодаря виртуализации исполнения файла, и обнаруживать вирусы.

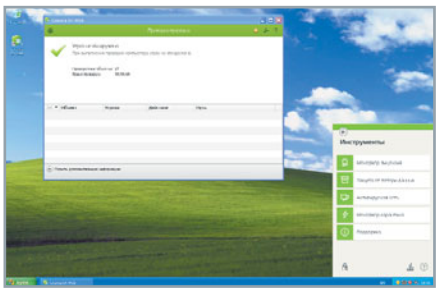
Технология *Origins Tracing* позволяет сканировать исполняемый файл и рассматривать его как обобщенный «портрет» угрозы. После теста система выполняет сравнение полученного образа с базой известных паттернов, что позволяет с высокой долей вероятности распознавать любые, в том числе неизвестные вирусы.

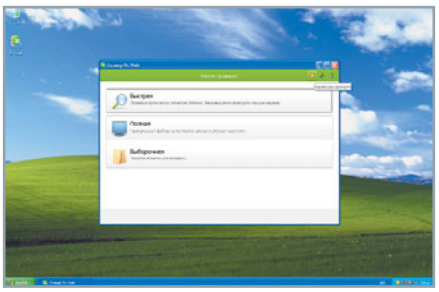
Dr.Web Security Space 10.0

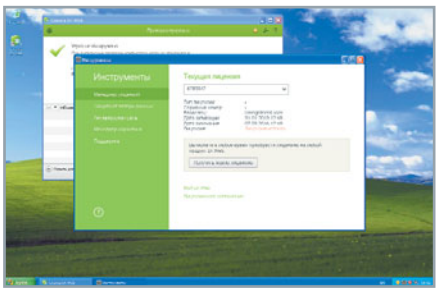
Рекомендуемая изготовителем цена: 1290 руб. (1 ПК + 1 мобильное устройство в год), 1600 руб. (2 ПК + 2 мобильных устройства в год), 2340 руб. (3 ПК + 3 мобильных устройства в год) за электронные версии.
«Доктор Веб», *www.drweb.com*

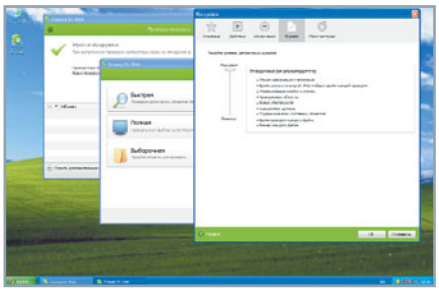
●●●●●

Достоинства. Надежность защиты, простой, без излишеств, интерфейс, масса технологий, гарантирующих безопасность ПК, минимальное влияние на быстродействие.
Недостатки. Не выявлены.









Еще один метод для выявления неизвестных угроз — *анализ структурной энтропии*. Он помогает обнаруживать их, выявляя характерные особенности расположения участков кода в проверяемых объектах, защищенных криптоупаковщиками.

Технология *ScriptHeuristic* предотвращает исполнение вредоносных сценариев в браузере и PDF-документах, не нарушая при этом функциональности легитимных сценариев. Она защищает также от заражения неизвестными вирусами через Web-браузер, работает независимо от состояния вирусной базы и совместима с любыми программами, использующими доступ к Интернету.

Конечно, не забыт и традиционный *эвристический анализатор*. Он содержит механизмы обнаружения неизвестных вредоносных программ и выявляет их путем нахождения характерных для вирусного кода признаков.

Пакет Dr.Web Security Space 10 сертифицирован ФСТЭК России, ФСБ России, МО РФ.

Каждому из признаков система самостоятельно назначает собственный «вес», указывающий степень важности угрозы. Гипотеза о распознании вируса срабатывает, когда суммарный набранный весовой коэффициент переходит за заданный предельный уровень. Таким образом, система оказывается способной не только отыскивать самые сложные вирусы, но ее можно настроить с учетом характера эксплуатации защищаемой компьютерной системы.

Еще одна технология в новой антивирусной системе защиты — *эмуляция исполнения программного кода.* Она позволяет обнаруживать полиморфные и сложношифрованные вирусы, когда непосредственный поиск по контрольным суммам невозможен либо затруднен. Такие ситуации могут возникать, например, из-за невозможности построения надежных сигнатур. Идея метода состоит в том, что система имитирует исполнение анализируемого кода, но выполняет его в защищенном эмуляторе, что локализует вредоносное действие и не дает ему распространиться в компьютерную систему.

Антивирус сегодня нельзя рассматривать как защиту для изолированной системы. Он — часть общей системы, которую получает пользователь в виде программных средств на его компьютере и подключаемых внешних сервисов. В рамках «Родительского контроля» и антивируса SpIDer Gate в пакете Dr.Web Security Space реализован сервис Dr.Web Cloud, позволяющий проверять запрашиваемые URL-адреса на серверах компании «Доктор Веб». Алгоритм работы прозрачен для пользователя: при попытке перехода на Web-сайт его URL-адрес сначала отправляется для проверки на серверы компании «Доктор Веб». Проверка выполняется в режиме реального времени, при этом никакой персональной информации, позволяющей идентифицировать пользователя, не передается, а пользователь получает более высокий уровень защиты, которая создается благодаря мощному алгоритмическому механизму и вычислительным ресурсам, предоставляемым разработчиком на стороне своих облачных серверов.

Соответствие нормативным российским документам сегодня стало таким же базовым требованием, как техническая поддержка и своевременная актуализация баз вирусных сигнатур. Система Dr.Web Security Space — российская разработка, которая полностью соответствует требованиям Федерального закона № 152-ФЗ «О персональных данных». Это касается не только защиты от несанкционированного доступа, но также является гарантией получения пользователем централизованной защиты каналов передачи данных.

Новая система сертифицирована на соответствие требованиям ФСТЭК России, ФСБ России, МО РФ. Ее можно использовать в сетях с повышенными требованиями к уровню защищенности. PC