Dr.WEB®
с 1992 года

Как выбрать антивирус

Методика выбора средств антивирусной защиты

Владельцам бизнеса, руководителям ИТ-департаментов предприятий и организаций, а также специалистам по антивирусным системам защиты предприятий

Dr.WEB®
с 1992 года

Содержание

Введение

В настоящее время на рынке достаточно предложений антивирусного программного обеспечения. Казалось бы, выбрать лучшее просто — нужно ориентироваться на победителей антивирусных тестирований, тем более что в лидерах тестирований зачастую встречаются даже бесплатные решения — замечательная возможность сэкономить! Но если бы всё было так просто...

- Здравствуйте, словили шифровальщика, антивирус ... не помог.
- Здравствуйте, ув. команда Dr.Web, помогите расшифровать зараженный компьютер вирусом WannaCry. Заражение произошло при открытии сайтов (какой именно сайт — не имею понятия, так как не сразу заметил, что произошло заражение), антивирус стоял ...

Многоточия в приведенных цитатах заменяют названия антивирусов, пользователи которых обратились в компанию «Доктор Веб» за расшифровкой в результате заражения троянцем Wanna Cry — эпидемии, поразившей даже крупнейшие компании.
Добавим к этому, что описания используемых антивирусом для обнаружения вредоносных программ технологий напоминают магические заклинания, и проблема выбора решения, которое на самом деле защищает, действительно становится проблемой.

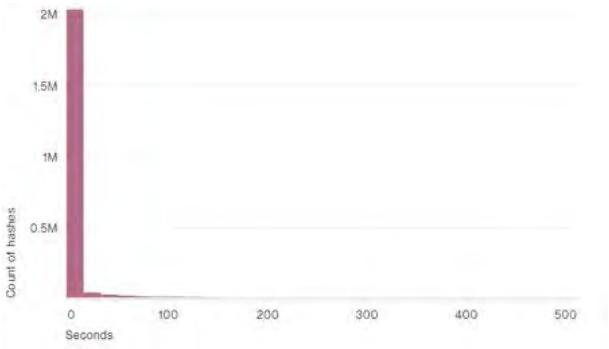
I. Основные причины заражения и меры противодействия

Практически каждый день в средствах массовой информации сообщается о заражении самых различных компаний и организаций. Иногда сообщается о многомилионных убытках. Большинство из этих компаний на момент заражения использовали антивирус. Почему так происходит?

1. Злоумышленники имеют возможность автоматизировать разработку вредоносных программ, в результате чего количество образцов вредоносных программ, поступающих в день на анализ в компанию «Доктор Веб», достигает миллиона!

- Необходимость оперативного добавления новых правил в антивирусные базы, базы правил файервола и превентивной защиты приводит к их замусориванию, в связи с чем компания «Доктор Веб» проводит регулярную очистку этих баз от дублирующих записей без потери качества детектирования.
- Уникальной особенностью антивирусных баз Dr.Web является алгоритм поиска сигнатур в антивирусных базах, базах правил брандмауэра и поведенческого анализатора, не увеличивающий время поиска при увеличении количества записей.

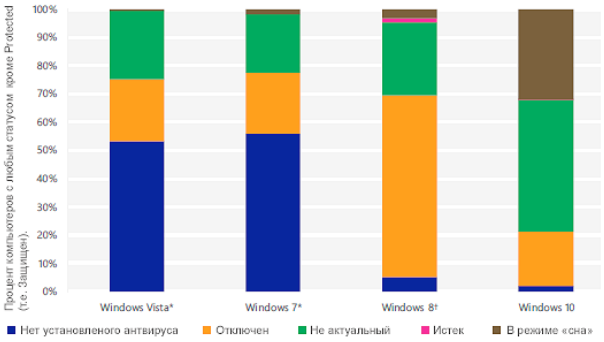
Антивирус не должен тормозить!



Более 99% образцов вредоносных программ (hashes) «живут» 58 секунд и меньше!

2. Пользователи антивирусных средств защиты не обновляют их или вообще отключают после установки.

- Статистика проверки компьютеров утилитой экстренной проверки Dr.Web CureIt! показывает, что до 60% компьютеров не защищены в достаточной мере.
- Почти 30% пользователей бесплатной версии утилиты Dr.Web CureIt! – пользователи встроенного в ОС Windows 7 и 10 антивируса Microsoft Windows Defender.



Рейтинг угроз

Период: неделя ; 10 строк

Название	Класс	%
DFH:HOSTS.corrupted	virus	6.73
Program.MediaGet.142	riskware	2.54
Program.Unwanted.1183	riskware	2.21
Trojan.InstallCore.2896	virus	1.24
Program.Unwanted.276	riskware	1.17
Adware.Zaxar.62	adware	1.08
Program.Unwanted.2	riskware	1.02
Program.Unwanted.1678	riskware	0.86
Program.Zona.86	riskware	0.75
Adware.Elemental.1	adware	0.69

Всего: 524508

Статистика проверки компьютеров утилитой Dr.Web CureIt!

Dr.Web находит угрозы!

3. Пользователи антивирусных средств защиты игнорируют предупреждения системы защиты, настраивают ее так, что вредоносные файлы, поступая в систему, не проверяются антивирусом. ▪ Одной из основных причин заражения компьютеров является исключение пользователями из антивирусной проверки программ, имеющих выход в сеть Интернет, и целых дисков компьютера. ▪ Еще один способ понижения уровня защиты антивируса — понижение уровня защиты компонента Превентивная защита.	**! Большинство заражений происходит в результате действий сотрудников компаний, их клиентов или партнеров.**
4. В локальных сетях подолгу не устанавливаются обновления и разрешены к использованию уязвимые сервисы. ▪ Эксплойты, с помощью которых происходит внедрение в атакуемую систему, рассчитаны на уязвимости, найденные до трех лет назад и ранее! Фактически время доступности уязвимости совпадает со временем жизни операционной системы! ▪ Шифровальщик WannaCry распространился с помощью эксплойта к уже закрытой Microsoft уязвимости!	

II. Требования к используемым средствам защиты

Антивирусная система защиты должна:

1. **иметь возможность обнаружения ранее неизвестных вредоносных программ.** Вирусописатели широко используют тестирование своих «произведений» на специализированных сервисах, в результате чего наличие в антивирусе только эвристических механизмов не позволяет гарантировать обнаружение новейших вредоносных программ. Наиболее часто средством сокрытия уже известных сигнатур является перепаковка ранее созданных вредоносных программ, в том числе с использованием упаковщиков с неизвестными системе защиты форматами. Для противодействия данному методу в решениях Dr.Web используются технологии, имеющие возможность поиска известных вредоносных программ в перепакованном виде (**Dr.Web Fly-Code**), а также проактивные средства защиты, определяющие характерные для вредоносных программ модели поведения и не требующие знания их сигнатур (**Превентивная защита Dr.Web**).

2. **иметь надежную систему самозащиты**, не позволяющую ее отключить как новейшим вредоносным программам, так и сотрудникам, желающим обойти действующие в компании правила безопасности. Наличие такой системы позволяет антивирусным решениям противостоять атакам вредоносных программ до момента получения обновлений, блокирующих источник атаки.

3. **иметь возможность блокировки отключения антивирусной защиты**. Для этого необходимо использовать централизованную защиту с возможностью ограничения прав пользователей в зависимости от выполняемых ими должностных обязанностей, а также защиту паролем доступа к настройкам системы защиты на станциях, не имеющих централизованного управления.

4. **поддерживать актуальность обновлений**. Система обновлений Dr.Web использует серверы, размещенные по всему миру. Технологии обновления позволяют обновить все станции защищаемой системы одновременно, без нагрузки для локальной сети. Использование централизованной защиты позволяет обновлять станции сети по расписанию и удаленно перезагружать станции, а защита паролем доступа к настройкам системы защиты на станциях, не имеющих централизованного управления, исключает возможность отказа от обновлений.

5. **поддерживать актуальность лицензии**. В продуктах Dr.Web действует система автоматического продления лицензий вашим поставщиком средств антивирусной защиты.

III. Выбор мер защиты

Антивирусная система защиты должна не только блокировать известные вредоносные программы, но и препятствовать распространению неизвестных вредоносных программ по сети и за ее пределы.

1. Должны быть защищены узлы локальной сети, на которые возможна установка антивируса, — в том числе операционные системы типа Linux и Mac, почтовые серверы, шлюзы сети Интернет, мобильные устройства. При использовании сотрудниками личных устройств и домашних компьютеров они также должны защищаться. В случае отказа от защиты личных мобильных устройств и компьютеров должны защищаться почтовые серверы и шлюзы сети Интернет, через которые сотрудники попадают к сервисам компании.
2. Системы, на которые возможно проникновение вредоносных программ (в том числе принтеры), но установка на которые антивирусных систем невозможна, должны быть максимально изолированы от остальной локальной сети.

Используемое средство антивирусной защиты рабочих станций должно:
1) уметь лечить вредоносные программы не только в момент их проникновения в систему, но и уже запущенные вредоносные программы — ранее неизвестные;
2) обнаруживать известные образцы вредоносных программ, упакованные в файлы с неизвестным форматом;
3) иметь возможность применения дополнительных механизмов (кроме сигнатурных и эвристических) для обнаружения неизвестных вредоносных программ — в том числе превентивной защиты и облачных компонентов;
4) включать в себя с целью защиты от проникновения неизвестных на момент заражения вредоносных программ:
   - персональный брандмауэр, обеспечивающий невозможность сканирования локальной сети, а также защиту от внутрисетевых атак;
   - систему ограничения доступа к сменным носителям и внутрисетевым ресурсам, в том числе сменным дискам, каталогам и интернет-сайтам;
   - централизованную систему периодического сканирования на отсутствие неактивных вредоносных программ и известных уязвимостей;
5) проверять все поступающие из локальной сети файлы до момента получения их используемыми приложениями, что исключает использование вредоносными приложениями неизвестных уязвимостей данных приложений;
6) иметь систему самозащиты, не позволяющую неизвестной вредоносной программе нарушить нормальную работу антивируса — антивирусное решение должно нормально функционировать до поступления обновления, позволяющего пролечить заражение;

7) иметь систему сбора информации, позволяющую максимально быстро передавать в антивирусную лабораторию всю необходимую для решения проблемы информацию. Должны быть исключены ситуации, когда в каждом случае заражения необходимую информацию нужно собирать вручную — в том числе и на удаленных рабочих станциях и серверах;
8) полностью размещать используемые антивирусные базы в оперативной памяти в целях исключения их подгрузки (в том числе монтирования) с жесткого диска, вызывающего торможение операций антивирусной проверки;
9) обеспечивать многопоточную проверку, исключающую образование очереди проверяемых файлов;
10) функционировать на операционных системах, уже не поддерживаемых их производителем;
11) для защиты от неизвестных вредоносных программ, передаваемых в почтовых сообщениях, использовать антиспам (антифишинг), не требующий постоянного дообучения;
12) исключать необходимость ручной настройки параметров загрузки процессора, используя систему автоматического анализа его загрузки.

Используемая система централизованного управления антивирусной защитой должна:
1) подобно системе обновления антивирусного решения: быть независимой от соответствующих механизмов, используемых в операционных системах; быть включенной в систему самозащиты антивируса, что позволяет исключить возможность перехвата системы обновления вредоносной программой. Недопустимо использование антивирусом системных компонентов, не помещаемых под защиту системы самозащиты антивируса;
2) использовать на всех рабочих станциях и серверах антивирус, включающий проактивный поведенческий анализатор и персональный файервол;
3) обеспечивать максимально быстрое получение обновлений защищаемыми рабочими станциями и серверами — в том числе по решению администратора, в ущерб общей производительности защищаемой локальной сети. Минимизация времени получения обновления должна в том числе обеспечиваться минимизацией размера самих обновлений, а также постоянным соединением защищаемых рабочих станций и серверов с сервером обновлений;
4) иметь возможность применения индивидуальных настроек для групп и отдельных пользователей;
5) иметь возможность полной или выборочной антивирусной проверки узла сети на наличие вирусных угроз как по команде пользователя или администратора, так и по расписанию;
6) иметь возможность централизованной установки, обновления и настройки программных средств антивирусной защиты, в том числе на недоступных с сервера узлах сети;
7) иметь возможность функционирования в сетях, разделенных на отдельные сегменты.

Дополнительно к использованию антивируса рекомендуется:

1. Ввести ограничения прав пользователей. В том числе:
   1) отказаться от использования прав администратора на рабочих станциях;
   2) ограничить права доступа к локальным и сетевым ресурсам;
   3) ограничить использование сменных устройств. В данном случае необходимо учесть, что белые списки устройств, как правило, неэффективны из-за того, что идентификаторы всех устройств партии совпадают.
2. Использовать разделение локальной сети на отдельные изолированные сегменты с установкой системы фильтрации трафика между ними.
3. Удалять неиспользуемые продукты, сервисы и компоненты.
4. Использовать систему резервирования, размещенную на отдельном сервере.
5. Вынести базы данных на отдельные серверы с запретом доступа к ним и использовать версионирование хранимых файлов и документов.
6. Ввести запрет на доступ в сеть Интернет и локальную сеть всем программам, кроме разрешенных.
7. Запретить использование доменных паролей администраторов на рабочих станциях.
8. Использовать централизованную установку всех обновлений безопасности для всех используемых продуктов. Обновлять регулярно все ПО, установленное на станциях.

Для экстренной проверки потенциально зараженных станций должен использоваться сетевой антивирусный сканер, а также загрузочный антивирусный диск / сменный носитель.

IV. Dr.Web Enterprise Security Suite — комплекс продуктов для бизнеса

Для корпоративных клиентов компания «Доктор Веб» предлагает свой флагманский продукт – комплекс Dr.Web Enterprise Security Suite, который обладает множеством уникальных возможностей:

- централизованная защита всех узлов сети – рабочих станций, почтовых, файловых серверов и серверов приложений, включая терминальные, интернет-шлюзов и мобильных устройств;
- комплексная защита рабочих станций от большинства существующих угроз благодаря наличию встроенных антивируса, антиспама, веб-антивируса, брандмауэра и офисного контроля;
- минимальная совокупная стоимость внедрения по сравнению с конкурирующими программами благодаря возможности развертывания серверов как под Windows, так и под Unix, встроенной базе данных, простоте установки и надежности защиты. Вместе с Dr.Web Enterprise Security Suite компании не придется приобретать дорогостоящее оборудование;
- возможность установки агентской части на уже зараженную машину и высокая доля вероятности излечения;
- минимальное использование ресурсов компьютеров и серверов благодаря компактности антивирусного ядра и использованию в нем новейших технологий;
- высокая эффективность обнаружения угроз, включая еще не известные вирусы;
- управление всей инфраструктурой защиты сети с одного рабочего места (через Веб-администратора), где бы оно ни находилось;
- реализация необходимых для конкретного предприятия и отдельных групп сотрудников политик безопасности;
- назначение отдельных администраторов для различных групп, что позволяет использовать Dr.Web Enterprise Security Suite как в компаниях с повышенными требованиями к безопасности, так и в многофилиальных организациях;
- настройка политик безопасности для любых типов пользователей, включая мобильных, и для любых станций – даже отсутствующих в данный момент в сети – позволяет обеспечить актуальность защиты в любой момент времени;
- защита любых сетей, в том числе не имеющих доступа в Интернет;
- возможность использования большинства существующих баз данных. При этом в качестве внешних могут выступать Oracle, PostgreSQL, Microsoft SQL Server, любая СУБД с поддержкой SQL-92 через ODBC;

- возможность самостоятельного написания обработчиков событий, что дает прямой доступ к внутренним интерфейсам Центра управления;
- наглядность системы контроля состояния защиты, непревзойденный по эффективности и удобству поиск станций сети;
- возможности выбора списка обновляемых компонентов продукта и контроля перехода на новые версии позволяют администраторам устанавливать только необходимые и проверенные в их сети обновления.

В состав комплекса Dr.Web Enterprise Security Suite входят следующие продукты:

Dr.Web Desktop Security Suite – защита рабочих станций, клиентов терминальных серверов, клиентов виртуальных серверов и клиентов встроенных систем

Dr.Web Server Security Suite – защита файловых серверов и серверов приложений (в том числе виртуальных и терминальных серверов)

Dr.Web Mail Security Suite – защита почты

Dr.Web Gateway Security Suite – защита шлюзов

Dr.Web Mobile Security Suite – защита мобильных устройств

Dr.Web Enterprise Security Suite внесен в Реестр отечественного ПО и позволяет выполнить все требования современного законодательства в области антивирусной защиты.

Все продукты в составе Dr.Web Enterprise Security Suite можно использовать бесплатно в течение 30 дней. Приглашаем компании сделать запрос демолицензии и оценить надежность защиты и качество детектирования и лечения Dr.Web.

Описание: https://products.drweb.ru/enterprise_security_suite

Запрос демо: https://download.drweb.ru/demoreq/biz/v2

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Антивирусная защита Dr.Web позволяет информационным системам клиентов эффективно противостоять любым, даже неизвестным угрозам.

«Доктор Веб» стал первой компанией, предложившей на российском рынке инновационную модель использования антивируса в качестве услуги, и по сей день продолжает оставаться безусловным лидером российского рынка интернет-сервисов безопасности для поставщиков ИТ-услуг. Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а

Тел.: +7 (495) 789–45–87 (многоканальный)

Факс: +7 (495) 789–45–97