Dr.WEB®

с 1992 года

Мифы об антивирусах

Dr.WEB®
с 1992 года

Мифы об антивирусах

Практически каждый современный пользователь компьютера или мобильного устройства сталкивался с последствиями действия вредоносных программ, ну или хотя бы читал либо слышал о таких последствиях. Но при этом «все знают» (т. е. верят), что «вирусы пишут разработчики антивирусов», «для Linux и Mac вредоносных программ нет», а «на Android вирус может установить по глупости только сам пользователь». Так ли это?

Вера в мифы, нежелание воспринимать объективную информацию и делать из нее правильные выводы, отказ признать факты и самообман в их отношении – все это ведет к опасным заблуждениям.

Следование заблуждениям влияет на принятие решений, которые могут оказаться неправильными, а иногда и приводить к тяжелым последствиям.

Эта брошюра посвящена мифам, окружающим антивирусы, причинам их возникновения и их влиянию на информационную безопасность каждого пользователя антивируса.

Миф № 1. Вирусов не существует

Это не так, но здесь важно различать собственно вирусы, способные размножаться самостоятельно, и прочие вредоносные программы. Вирусы существуют, но их крайне мало по сравнению с распространенными сейчас троянцами.

Вирусами в строгом определении этого термина называются только те вредоносные программы, которые имеют механизм саморазмножения, — т. е. обладают возможностью создания своих копий и внедрения своего кода в другие файлы.

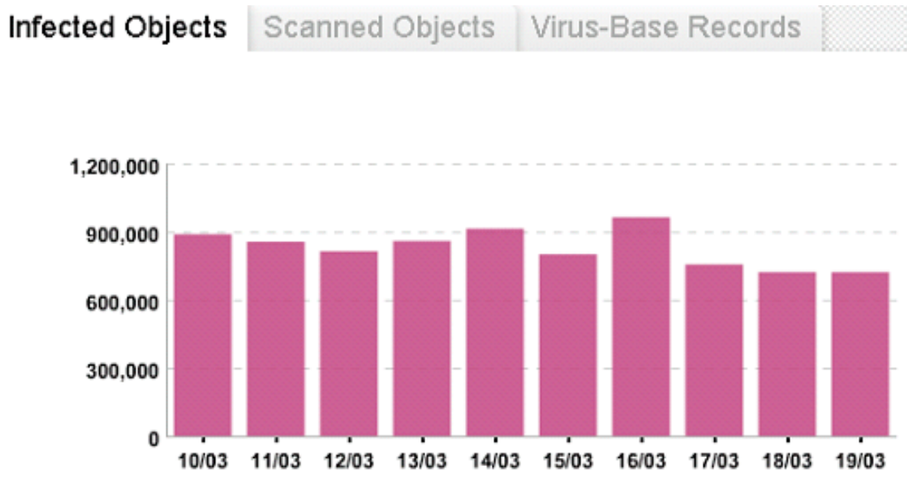
На сегодняшний день подавляющее большинство вредоносных программ (более 90%) — троянцы. Они не имеют механизма саморазмножения и не являются вирусами.

Миф № 2. Новые вредоносные программы появляются редко

Даже некоторые IT-специалисты уверены, что количество создаваемых в день вредоносных программ — порядка ста. На самом деле это далеко не так.

В антивирусные лаборатории поступает до двадцати пяти миллионов потенциально вредоносных образцов в месяц.

График поступления образцов на анализ в антивирусную лабораторию «Доктор Веб» в марте 2015 года

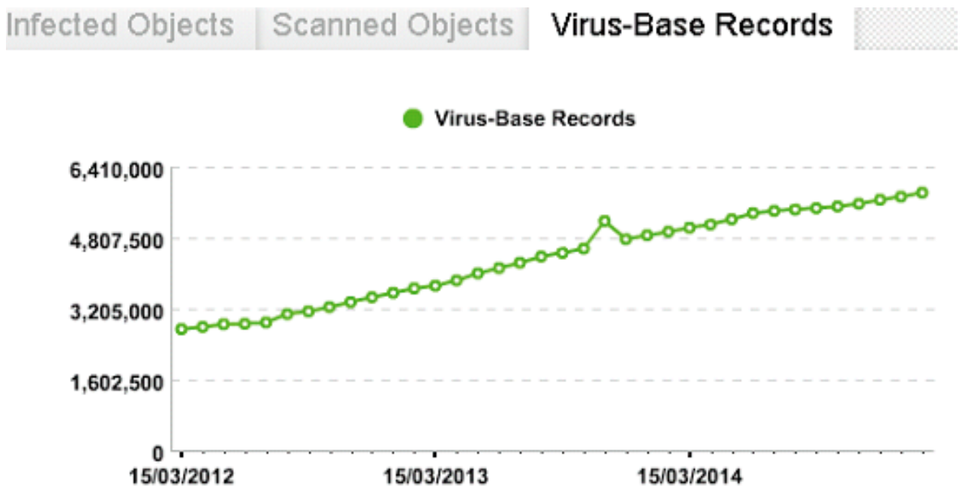


Не все пришедшее — вредоносные программы. И конечно, некоторые образцы повторяются. Но все они должны быть обработаны нашими специалистами.

Обработать несколько миллионов образцов в месяц вручную – нереально.

Большинство образцов обрабатывают специализированные роботы. Вирусные аналитики исследуют только сложные образцы, автоматическая обработка которых невозможна. Вирусная база Dr.Web растет ежечасно.

График роста количества записей в вирусной базе Dr.Web



Миф № 3. Антивирусные компании сами пишут вредоносные программы

Немало пользователей убеждено, что вирусы пишут сами разработчики антивирусов, т. к. им это выгодно — ведь если не будет вирусов, пользователи не будут покупать антивирусы.

Это – наш любимый миф! И самый живучий из всех мифов об антивирусах. Не проходит и месяца, чтобы кто-то не написал нам о нем через форму обратной связи.

Миф логически вырастает из «знаний» о том, что:

1. количество создаваемых в день вредоносных программ крайне невелико,
2. их по силам написать нескольким специалистам,
3. которые работают, конечно же, в антивирусных компаниях.

- Число разрабатываемых злоумышленниками вредоносных программ настолько велико, что антивирусные лаборатории и так загружены работой в три смены по 7 дней в неделю. Писать вредоносные программы при этом и вовсе лишено смысла, справиться бы с тем, что приходит на анализ извне.
- Создавать вредоносную программу для специалиста по информационной безопасности – занятие абсолютно бессмысленное, прежде всего, потому, что если детект этой троянской программы будет добавлен в базы разрабатываемого им же антивируса, пользователи будут защищены от такой угрозы с самого начала, а спустя очень короткое время этот троянец попадет в базы и других антивирусных программ. Зачем впустую тратить время?
- Создание вредоносного ПО – уголовно наказуемое преступление. Если станет известно, что кто-то разрабатывает вирусы, этот человек рискует оказаться за решеткой. И об этом обязательно станет известно – у вирусных аналитиков достаточно недоброжелателей.
- Антивирусные вендоры не только не пишут вирусов, они даже не рассылают уже известные вредоносные файлы в целях тестирования, о чем периодически нас просят клиенты, желающие протестировать новое ПО, и журналисты, желающие провести сравнение. Если когда-нибудь станет известно о том, что компания или ее сотрудник занимались созданием или просто распространением вредоносного ПО, на бизнесе этой компании можно будет поставить крест.
- Многие производители средств антивирусной защиты — и в их числе компания «Доктор Веб» — не принимают на работу тех, кто так или иначе занимался хакерством. Человек, который когда-либо занимался созданием вирусов, имеет низкий уровень морали.

Кто на самом деле пишет вредоносные программы?

На заре компьютерной эпохи вредоносные программы создавались действительно преимущественно с целью «пробы пера» и самовыражения. И сейчас бывает, что вредоносные программы пишут одиночки, желающие славы, но основную опасность представляют не они.

Современные вредоносные программы разрабатываются не просто вирусописателями-профессионалами. Их разработка – часть хорошо организованного криминального бизнеса.

В состав криминальных группировок входят:

- Организаторы — лица, которые налаживают процесс создания и использования вредоносного ПО, а также руководят им.
- Разработчики вредоносного ПО.
- Тестировщики созданного ПО.
- Исследователи – специалисты по поиску пригодных для преступного использования уязвимостей в операционных системах и прикладном ПО.
- Распространители вредоносного ПО.
- Администраторы, обеспечивающие распределенную безопасную работу внутри преступного сообщества и управление бот-сетями.
- Веб-мастера, создающие сайты для распространения вредоносного ПО.
- Менеджеры, занимающиеся реализацией вредоносных программ (некоторые троянцы пишутся на продажу иди для сдачи в аренду).
- Организаторы DDoS-атак.
- Создатели недобросовестных рекламных ресурсов и партнерских программ, зарабатывающие на рекламных троянцах.

Благодаря четкой организации криминальных групп, занимающихся разработкой и распространением вредоносных программ, их производство поставлено на поток. Это обеспечило взрывной рост числа создаваемых злоумышленниками вредоносных программ и не замедлило сказаться на количестве ежедневных сигнатурных записей, добавляемых в вирусные базы.

Число программ, выпускаемых одной группировкой, может достигать сотен образцов в день — и ни один из них некоторое время после выпуска не будет обнаруживаться антивирусным ПО, используемым целевой группой жертв. Почему так происходит – мы объясним дальше.

С какой целью пишут вредоносные программы?

Вредоносное ПО создается исключительно с целью извлечения выгоды.

Тот, кто вовлечен в процесс создания, распространения и поддержки инфраструктуры для функционирования троянца, созданного для хищения чего-либо, — преступник.

Современные троянцы воруют как информацию, так и материальные активы пользователей и компаний. Для последующей перепродажи сгодится все украденное:

- Логины и пароли — к системам онлайн-банкинга и электронных платежей, аккаунтам в социальных сетях и т.д.
- Виртуальные деньги (например, биткойны).
- Письма электронной почты и адреса книги контактов.
- Фотографии — с их помощью можно шантажировать жертву или нанести ей моральный ущерб, выложив снимки в Интернете.
- Любого рода техническая информация о ПК жертвы.
- Игровые аккаунты и артефакты.

Даже если на компьютере нечего украсть — он сойдет для создания ботнета.

Внимание!

В некоторых странах владелец компьютера, вовлеченного в бот-сеть с целью атак на другие компьютеры или сайты, может быть привлечен к уголовной ответственности — даже если он не знал об этом.

Миф № 4. Антивирус обязан обнаруживать все вредоносные программы в момент их проникновения

Это поразительно живучий миф. Но это требование просто невыполнимо! Также как невозможно изобрести лекарство сразу от всех болезней. Панацеи не существует, и с этим придется смириться, хотя о ней веками мечтают люди.

Миф существует в силу того, что большинству пользователей неизвестно, как организован преступный бизнес вирусописателей. Одним из главных процессов в создании «хорошего» троянца (т. е. незаметного для пользователя и его антивируса) — является процесс его **тестирования на необнаружение** большинством популярных антивирусов.

Только никем не определяемый троянец выпускается в живую природу или внедряется на ПК жертвы, если атака целевая.

Вот и получается, что существует временная дельта между выпуском троянца злоумышленниками, попаданием его образца на анализ в антивирусную лабораторию и изготовлением противоядия. Правда, это относится только к действительно сложным и «успешным» троянцам. Большинство заурядных вредоносных программ детектируется сигнатурно, а также эвристическими и другими несигнатурными технологиями антивирусного ядра Dr.Web.

Миф № 5. Действие вируса на компьютере всегда заметно

Этот миф – из наиболее опасных! Он уходит корнями во времена написания первых вирусов, большинство из которых были либо деструктивными (несли разрушительные функции, например, уничтожали всю информацию на ПК), либо сопровождали свое существование на зараженной машине бурной деятельностью — например, массовой рассылкой писем со своей копией, что замедляло работу системы и было заметно.

Сегодня цели злоумышленников — ваши деньги и ваши данные. Чтобы украсть больше, нужно сидеть тихо.

Кстати:

1. Некоторые вредоносные программы после заражения устраняют уязвимости в системе, через которые могут проникнуть иные вредоносные программы, и очищают систему от уже проникших конкурирующих вредоносных программ.

2. Некоторые троянцы «убивают» антивирус (завершают соответствующие процессы в системе), а потом помещают значок антивируса в Область уведомлений Панели задач Windows, чтобы создать у пользователя впечатление, будто антивирус все еще работает, и усыпить бдительность. В ресурсах такой вредоносной программы предусмотрены значки всех популярных антивирусных решений, и умный троянец выбирает тот, который соответствует установленному на атакуемом ПК. Конечно, такой значок не реагирует на щелчки мышью и другие попытки воздействия, и кажется, будто антивирус «завис». По факту машина остается беззащитной. В Dr.Web реализована специальная система самозащиты от подобных атак.

Так что не обольщайтесь — вирусописатели давно поняли, что лучший троянец — незаметный для пользователя троянец.

Но миф до сих пор живуч как никакой другой.

А вот вера в него приводит к самым печальным последствиям. Верящие в этот миф люди либо не используют антивирус вовсе, либо не считают необходимым придерживаться элементарного правила использования антивируса, а именно — проводить регулярные сканирования.

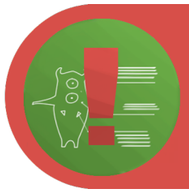
Миф № 6. Антивирус определяет вредоносные программы только по сигнатурам

Этот миф живет с первых лет существования антивирусов. Тогда, более 20 лет назад, он имел под собой основания.

Чисто сигнатурные антивирусы, т. е. определяющие вредоносные программы по записям в вирусных базах, вымерли в 90-х годах прошлого века, когда появились полиморфные вирусы, изменяющиеся при каждом запуске и, соответственно, не детектируемые по сигнатурам (кстати, именно это стало причиной появления российского антивируса Dr.Web).

Если бы и сегодня антивирус умел распознавать новые вирусы только на основании записей в вирусных базах, такие базы не смог бы уместить в своей памяти ни один компьютер, проверка занимала бы много времени, а быстродействие ПК было бы серьезно замедлено.

Сегодняшний антивирус — это комплекс эвристических, поведенческих и превентивных технологий несигнатурного характера, сочетание которых вместе с записями в вирусных базах позволяет антивирусу обеспечивать вашу безопасность от реальных угроз.



Миф № 7. Если для вредоносной программы в вирусной базе нет записи, антивирус обязан распознать ее с помощью эвристических технологий

Данный миф возник из заблуждения о том, что антивирус обязан распознавать 100% вредоносных программ, и поддерживается наличием тестов антивирусов на эвристический анализ.

Эвристики обнаруживают только новые модификации ранее попавших на анализ вредоносных программ, с уже известным антивирусу поведением.

Злоумышленники, разработавшие троянца, чтобы избежать необходимости его переделки при занесении информации о нем в вирусные базы антивируса, просто переупакуют его файловым упаковщиком или зашифруют.

Что делать в таком случае антивирусу? Можно добавлять каждый такой образец в вирусную базу (некоторые антивирусы, возможно, так и делают!), а можно ловить с помощью технологии FLY-CODE и технологии анализа структурной энтропии, как это делает Dr.Web. Первая обеспечивает проверку упакованных исполняемых объектов, распаковывает нестандартные упаковщики методом виртуализации исполнения файла, вторая обнаруживает неизвестные угрозы по особенностям расположения участков кода в защищенных криптоупаковщиками проверяемых объектах.

Антивирус обязан и не допускать заражения, и лечить от уже проникших вредоносных программ.

Как это ни печально, но антивирус не может обнаружить все вредоносные программы в момент заражения. Поэтому для предотвращения заражения на помощь антивирусу приходят иные системы — в том числе системы ограничения запуска неизвестных программ и контроля поведения.

А вот вылечить систему от уже проникших и активных вредоносных программ, противодействующих системам защиты в попытках их удаления, может только антивирус.

Ни один программный продукт, кроме антивируса, не способен вылечить зараженную систему от вредоносной программы. Лечение — миссия, доступная только антивирусу и никакому другому программному продукту.

Миф № 8. Для защиты от вредоносных программ помимо антивируса требуется иное ПО

Современный антивирус способен обнаруживать и шпионское ПО, и руткиты, ему не требуются дублеры в виде дополнительного ПО. Кроме того, в комплект поставки многих антивирусов включены брандмауэры (межсетевые экраны) – специальные компоненты, способные защитить компьютер от несанкционированного доступа по сети.

Антивирус находит и устраняет из системы любые типы вредоносных программ. Никакие иные программные продукты в помощь антивирусу не нужны.

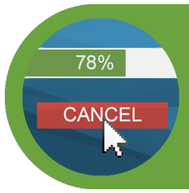
Кроме настоящих антивирусов существуют программы, выдающие себя за антивирусы или иное защитное ПО. Во многих случаях они не просто бесполезны, но еще и сами заражают тех, кто доверился рекламе.

Уязвимости в программных продуктах, социальная инженерия и уловки фишеров только увеличивают риск подцепить инфекцию без участия пользователя, какую бы осторожность он ни проявлял.

Например, именно уязвимости сыграли главную роль в масштабном распространении первой эпидемии для Mac OS X, которая произошла благодаря троянцу **BackDoor.Flashback.39**. Для его распространения злоумышленники использовали сразу несколько уязвимостей в виртуальной машине Java, в результате:

650 000 компьютеров Mac

были инфицированы **BackDoor.Flashback** по всему миру.



Миф № 9. Если не посещать подозрительные сайты и не переходить по ссылкам в письмах от незнакомых отправителей, антивирус не нужен

Верящие в то, что антивирус не нужен и только тормозит работу компьютера, полагают, что для заражения системы необходимо собственноручно установить троянца — например, скачав его по вредоносной ссылке из письма.

Однако практика показывает: в огромном количестве случаев пользователи сами скачивают и устанавливают на свой ПК троянца, даже не подозревая об этом!

Также существуют сценарии атак, когда пользователю не требуется предпринимать каких-либо действий для запуска троянца. Вы и ахнуть не успеете, как без вашего участия на ПК установится незаметный для вас троянец.

Миф № 10. Антивирус не нужен, если компьютер используется только для игр

Современная индустрия компьютерных игр представляет собой высокоразвитый рынок с ежегодным оборотом в десятки миллиардов долларов. И геймеры не застрахованы от интернет-угроз.

«Прокачивая» своих персонажей, добывая игровые артефакты, пользователи зачастую делают это за реальные деньги – и вот тут их могут ожидать неприятные «троянские» сюрпризы. Например, **Trojan.SteamBurglar.1** *способен красть игровые предметы с целью их последующей продажи.*

Помимо троянцев существует масса мошеннических способов заставить игрока расстаться с ценными артефактами и даже аккаунтом, сделать его ПК участником бот-сети, вовлеченным в DDoS-атаку на игровой сервер неугодной компании и т. д.

Картину дополняют троянцы-шифровальщики, выискивающие на ПК жертвы следы онлайн-игр или аккаунта в Steam и шифрующие файлы с требованием последующего выкупа.

Антивирус защитит от заражения подобными программами, а веб-антивирус SpIDer Gate не позволит зайти на мошеннический сайт.

Доверьте защиту ваших информационных ресурсов отечественному ПО

- Защита от рисков, связанных с изменением международной обстановки, — таких как отказ в использовании, продлении, поставке, получении обновлений
- Защита от угроз, созданных для целенаправленных атак на предприятия и граждан России
- Доступ к технической поддержке в России, на русском языке
- Сертификаты Министерства обороны Российской Федерации, лицензии ФСБ России и ФСТЭК России на проведение работ, связанных с государственной тайной

www.антивирус.рф

Dr.Web в каталоге «Отечественный софт»

Российской Ассоциации Разработчиков Программных Продуктов (АРПП)

http://www.arppsoft.ru/catalog/230

Мы являемся одним из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеем свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки, которые расположены в России.

Наши продукты	Наши клиенты
http://products.drweb.ru/biz	http://customers.drweb.ru

Со знаком качества

Dr.Web сертифицирован Министерством обороны Российской Федерации. Компания «Доктор Веб» имеет лицензии ФСБ России и ФСТЭК России на проведение работ, связанных с государственной тайной. Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

Все лицензии и сертификаты «Доктор Веб»

Перечень сертифицированных продуктов Dr.Web

Поставка версий Dr.Web, сертифицированных МО России, ФСБ России, ФСТЭК России

125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 7
Тел.: +7 495 789-45-87 (многоканальный)
Факс: +7 495 789-45-97

«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.

www.drweb.ru | www.av-desk.com | http://freedrweb.com | http://mobi.drweb.com