Антивирус — Lurkmore

К вашему сведению!

В этой статье мы описываем само явление антивирусов, а не составляем списки холиваров. Ваше мнение о фичах Касперского, Нода и прочих здесь никому не интересно, поэтому все правки с упоминанием тем для холивара будут откачены, а их авторы — расстреляны на месте из реактивного говномета, for great justice!

I see what you did there.

Информация в данной статье приведена по состоянию на середину-конец нулевых. Возможно, она уже безнадёжно устарела и заинтересует только слоупоков.

Антивирус — программа, делающая вид, что ищет вирусы, трояны, червиё и прочую заразу в иммунодефицитной среде Microsoft® Windows®, но в реальности не делает ничего, замедляя работу девайса, на который установлена, в отдельных случаях вызывая сбои работающих программ. Пытается защищать от угроз, которых нет в антивирусных базах, но хреново умеет это делать. Используется и на серверных nix-системах, но гораздо реже и для более специфических целей. Выступает как средство для выколачивания денег из организаций, которыми руководят быдлоадмины, неспособные настроить информационную систему компании для защиты от вирусов и всяческих недалёких личностей.

Download now!

Ликбез

Первые вирусы писались мозговитыми затейниками (в те далёкие времена их звали хакерами, в благороднейшем из смыслов) из инженерных институтов. Естественно, писались они исключительно во имя добра, ради лулзов и отработки некоторых математических и логических моделей.

Суть первых вирусов сводилась к нестандартному использованию логических схем компьютера и инициированию сбоев и смятения в его тонкоорганизованной электронной душе. О массовом заражении компьютеров и речи не шло — не было массовой компьютеризации. В дальнейшем вирусы писались опять же ради лулзов, передавались через дискеты и прочие носители, но до массовости опять же не доходило.

С появлением сетей, а позже и интернетов, работы у вирусописателей прибавилось, да и лулзы начали всё больше походить на профит. Коды стали сложнее, появились способности к самоизменению (полиморфизму).

Сейчас вредоносное ПО пишется всё больше для извлечения профита: зомби-сети (ботнеты) для рассылки спама и DDoS-атак, инструменты для кражи конфиденциальной информации с целью выкупа или продажи конкурентам, вывод оборудования конкурента из строя и т. п.

Разумеется, к тому моменту как количество активных вирусов в цифровом пространстве начало стремительно возрастать, некоторые вирусописатели начали задумываться о противодействии вирусным атакам и извлечении профита.

Создание антивируса

- Берём свой самый лучший вирус;
- Отрезаем от него вредоносную составляющую, опционально пришиваем полезную составляющую, анально огораживаем;
- Прикручиваем к нему базу данных с описанием других вирусов;
- Рисуем к нему интерфейс, логотип и называем его «Антивирус»
- Продаём. Требуем бабло каждые n дней;
- ??????
- PROFIT

Теперь можно заколачивать бабло не только на вирусах, но и на продаже противоядий от них. Всё гениальное просто.

Принципы работы антивируса

Для обнаружения вредоносного кода в софте, макросах, интернетах антивирусы используют такие методы как:

- **Сигнатурный метод обнаружения** — бесполезная в нынешних реалиях вундервафля. Вирус отлавливается, изучается, для него создается противоядие, результаты заносятся в реестр вирусов и в базу сигнатур. Сигнатуры скачиваются пользователями с очередным обновлением.

  Плюсы:

  - Надёжность метода. Новые вирусы разбирают на куски довольно быстро. Во время эпидемий это важно.
  - Быстродействие. Но скорее простота алгоритма проверки, нежели скорость.

  Минусы:

  - На каждый морф вируса нужна новая сигнатура. Базы растут с ужасающей скоростью, а скорость проверки при большой базе падает. Начинаются танцы, с тем чтобы оптимизировать сигнатуры и одной сигнатурой покрывать целое семейство вирусов, а это приводит к написанию эвристики. А эвристика приводит к ложным срабатываниям. Круг замкнулся.
  - Для того чтобы проанализировать вирус, нужно для начала его обнаружить. Да-да, та самая кнопочка «отправить на проверку», которая в том или ином виде есть в каждом диалоге обнаружения подозрительных файлов на компьютере пользователя. Хотя, конечно, на пользователей антивирусные компании особо не полагаются, а ищут вирусы в интернетах сами. Знающий человек вам скажет — те вирусы, что присылают пользователи, составляют 1% от общего «веса» антивирусной базы. В то время как основную массу вирусов антивирусные вендоры получают из облака, по обмену друг от друга и с платной части virustotal.com.

- **Эвристический метод обнаружения** — метод анализа поведения. Рекламируется как эффективное средство для обнаружения новых угроз, но в реальности вероятность обнаружения нового вредоносного ПО очень низкая или нулевая, если его пишет профессиональный вирусмейкер. Эвристический анализатор висит в памяти и отслеживает **все** действия системы. Если в порядке действий наблюдается нехорошая тенденция, то объект, ее вызвавший, помечается как подозрительный и анально огораживается до выяснения обстоятельств. Так обнаруживается некоторая часть новых вирусов и чуть больше половины полезного софта. Стоит заметить, что после выхода x64 версий Windows систем, ситуация изменилась: антивирус может мониторить лишь ничтожную часть действий ОС, ту что MS разрешил. Технология patchguard с одной стороны несколько усложнила жизнь малвари, а с другой — закрыла кислород антивирусам на перехват всех системных событий. Оставили возможность следить только за файлами, процессами и реестром.

  Плюсы:

  - Реагирование на угрозы, не занесённые в базу сигнатур.
  - Относительно высокая эффективность против не очень опытных вирусмейкеров.
  - Устойчивость к новым штаммам.

  Минусы:

  - Ложные срабатывания. Под условия поиска попадают почти все кряки и кейгены, кошерные кейлоггеры, программы удалённого администрирования (понятно, что без интернета они не могут работать) и т. п., даже если они иногда уже были дезинфицированы. Тут следует заметить, что эвристический анализ чаще всего срабатывает на упаковщике кода, ужимающего экзешник (kkrunchy, например) и обфускаторы. Зачем же жать программу в 20 строчек? Нет, не для того, чтобы туда влезла музычка! Код пакуется для того, чтобы школьник, не имеющий никакого представления о программировании, воскликнул: «Эй, да в эти 20 килобайт никогда не поместится ни один троян, и уж тем более руткит! Видно же, что всё занимает картинка и музычка! Ещё непонятно, как влезло!»
  - Страдает быстродействие. Пережёвывание всего, что происходит в памяти компьютера, помимо фоновой работы самого сканера файлов и висящих в памяти драйверов антивируса, жевания входящего трафика и полдюжины дополнительных свистоперделок вроде контроля целостности приложений, тормозит работу независимо от мощности комплектующих.

- **Брандмауэр** — он же фаерволл. Интересная вундервафля, контролирующая сетевую активность. Проверяет все UDP, TCP и прочую муть. Контролирует входящие и исходящие соединения.
  Входящие соединения: например, ваша любимая программа-сервер ожидает подключений извне и ждет, когда её хакнут через открытый порт. Если порт открыт, это ещё не значит, что программу-сервер смогут хакнуть, нужен подходящий эксплоит.
  Исходящие соединения — то, чем пользуются почти все программы. Они начинают соединяться первыми, потом начинают принимать и отдавать пакеты данных (байты). Что они там передают — известно только черту и создателю программульки. Если же запретить сие безобразие фаерволлом, то программы начнут «плакать» и писать, что интернета больше нет. Поэтому приходится разрешать,

и ваши персональные данные могут быть нагло спизжены. Чтобы было не так обидно, можно в фаерволле разрешать отправлять пакет данных только на определенный IP — любой программы, которая лезет обновляться только на свой сайт. Если персональные данные и спиздят, то их спиздит не кто угодно, а известный издатель.
В общем, программы хотят устанавливать и входящие, и исходящие соединения. Хотят они много, поэтому фаерволл много чего разрешает, а потому с настройками по умолчанию малополезен. В качестве основного минуса прописываем дурную привычку обращивать ПК «сосульками» (со временем замедлять работу).

- **Проактивная защита** — частный случай неправильного подхода к эвристике. «Легальный» вредоносный вирус, который перехватывает вызовы системных функций, мониторит обращение запущенных процессов к файловой системе, реестру, может нарушать нормальную работу ОС и выдавать окошки, мешающие работать. Способен выебать мозг пользователя в интерактивном режиме (когда юзер вершит суд над программой). В отличие от простого вируса, вымогает деньги за продление подписки. Вредоносные и невредоносные программы часто выполняют одни и те же действия, неопытному пользователю приходится разрешать почти всё или всё, дабы игрушка или любая другая хрень запустилась, в противном случае при запретах обычно всё накрывается к чертовой матери. К сожалению, проактивная защита только подозревает, что в этой программе страшный и ужасный троян, и без суда и следствия может приговорить её к расстрелу (если в настройках стоят запреты, либо в интерактивном режиме юзер запрещает что-либо).

- **Облачные технологии.** В последнее время антивирусы пытаются надавать пиздюлей вирусописателям и переходят на новые методы защиты. Количество вирусов свирепо растет. При таком темпе нынешние методы будут казаться детской забавой.
Работают технологии так. Какой-то файл появляется в инете, его запускают ламеры на своих компах, и вирус попадает в облако. Там записывается, сколько долбоёбов запустили этот файл. Чем больше ламеров запустят файл, тем быстрее остановят эпидемию. Облако собирает информацию — что происходит на компах ламеров — чем больше подозрительной активности, тем выше вероятность, что началась эпидемия трояна или червя. Другие ламеры узнают, что файл запускали столько-то людей и появился он тогда-то. Если файл появился в облаке вчера, то ламеру стоит задуматься — а надо ли рисковать и запускать это?

- **Номенклатура вирусов у антивирусов.** Каждая антивирусная лаборатория имеет свою номенклатуру вирусов (классификацию). По этой причине каждый антивирус выносит свой приговор файлу — может навредить, наверно навредит, точно не навредит. Fun в том, что один и тот же файл антивирусы могут обозвать совершенно разными обидными прозвищами — трояном, червем, бэкдором, рекламной программой, вредоносной, потенциально опасной или безопасной. Например, есть червь, который кочует с компа на флэшку (и наоборот) и файлы превращает в ярлыки. Но некоторые вирлабы называют его трояном.
У некоторых антивирусов есть дурная привычка называть всё подряд вредоносным ПО, трояном — даже безобидные кряки, кейгены и трейнеры. Многие вирлабы просто воруют детекты у других вирлабов, не проверяя, а не ошибся ли предыдущий оратор.
Вредоносное ПО — это такая программа, которая либо точно навредит, либо навредит, если сумеет. Например, троян-шифровальщик точно навредит, если вы по пьяни забыли сделать бэкап своих ценных файлов, или если троян нашел уязвимость в HIPS, или загрузил драйвер, работающий в режиме ядра (руткит) и стал хозяином в системе, и рассказывает байки антивирусу, что никаких угроз нет (в ядре у руткита и антивируса равные права). А если вы не храните информацию, которая принесет пользу злому хакеру, или настроенный HIPS смог героически защитить важные файлы, то троян-шпион соснет хуйцов и не спиздит ваши персональные данные.
У антивирусов тоже разногласия по этому поводу — навредит ли троян или обломается? Поэтому некоторые для перестраховки называют этот файл вредоносным ПО (троян, вирус, червь).
Потенциально опасное ПО — это Hacktool, Riskware, not-a-virus, Tool, Adware, Hoax и т. д. Это ПО, которое может причинить вред при неправильном использовании. У антивирусов же разногласия бывают часто. Половина антивирусов клянется, что эта программа навредит, другая половина — что эта программа может навредить при определенных обстоятельствах.
Невредоносное ПО — это программы, которые якобы безопасны. Не причиняют видимый вред хомячкам, но на самом деле могут иметь недокументированные возможности. Некоторые антивирусы любят повыпендриваться и писать, что эта программа подозрительна, или с трояном. Большинство других антивирусов при этом молчит, как рыба.

Avast!

Avast! (от англ. *Avast!*, дословно *«Стой!»*) — антивирус, разработанный и поддерживаемый чешской компанией Avast Software (до 1 июня 2010 года — ALWIL Software) на деньги чешской диаспоры.

> Люди, помогите, такая ситуация. Установил сегодня антивирус avast, почистил им систему, он удалил каких-то 3 системных файла, теперь:
>
> 1) при работе в интернет вместо букв на некоторых сайтах одни иероглифы видно; 2) на некоторых сайтах не могу зарегистрироваться, всё время пишет что код проверки введен неправильно. Подскажите, что делать и как это можно исправить?! Спасибо.

— *tehnari.ru*

Аваст — это антивирус, который состоит чуть менее, чем полностью из каких-то сканеров, которые, по словам разработчиков, должны проводить эвристический анализ всего, что есть у пользователя на компьютере. Сей продукт заслужил у хомячков, школоты и прочих статус православного за счет халявности.

Аваст борется с вирусами при помощи:

- Нежного металлического голоса, оповещающего об обновлении вирусной базы. Всю драму пользователь впервые может почувствовать, если оставит звук громко включённым, ибо неожиданный проигрыш сего музыкального файла часа в три ночи вызывает лёгкое недомогание. Можно убрать в настройках.
- Спизженным сигналом «Notify» перед каждым металлическим голосом из информаторов Питерского метро (или наоборот?).
- Анимированного шарика в трее. Этот шарик, по мнению Анонимуса, из той же оперы, что и меметичная Скрепочка из офиса Мелкомягких. В настройках шарик можно легко заменить на неподвижный. Или совсем убрать.

Участвуя в гонках антивирусов, Аваст доставлял баттхёрт своим ярым приверженцам, так как в настройках у него имелись режимы сканирования — быстрый, стандартный и тщательный. По умолчанию настройки установлены на «стандартный», и в этом «стандартном» режиме Аваст ловил вирусов даже меньше, чем в «быстром» (проверено электроникой). Сделано это, видимо, just for lulz. В новой версии добавлены новые виды сканирования.

Несмотря на недостатки, Avast 4.x успешно конкуририровал со всякими касперскими и прочими нодами, поскольку это один из самых быстрых и ненадоедливых антивирей, если его правильно сконфигурировать буквально парой кнопок (не считая уже упомянутой бесплатности).

С появлением же Avast 5.x показалось, что крах остальных антивирусных систем близок, поскольку новобранец ещё быстрее предшественника (можно тотально выключить проверку некоторых расширений в одном единственном меню), появилась песочница и прочие ништяки, которых так долго ждали (даже в домашней бесплатной версии). Да и Google выбрал официальным партнёром (на сервисах Google рекомендуют именно Avast), что какбе намекает. Тем не менее, попробуйте после полугода использования Аваста (в любых режимах) просканировать свой сундук с драгоценностями с помощью того же CureIt!. Особенно актуально для тех, кто активно ёрзает по всему интернету, а не посещает некий строгий перечень из проверенных/нужных для работы/просто интересных ресурсов.

В последней версии появилось жалкое подобие проактивной защиты — экран поведения.

После того как Крым перешёл под пяту РФ, аваст ввёл санкции против жителей полуострова.

В 2014 году хакеры взломали форумы Avast и украли данные почти полуляма юзверей.

Однако чем дальше, тем больше в антивирусе появлялось рекламы, разных не имеющих к защите отношения инструментов и прочих свистоперделок, что превращает его из годного продукта в унылое говно. Увы и ах.

Ахтунг!
Троянский конь!

Сканирование до
загрузки оси

Dr.Web

Доктор Веб — один из самых древних антивирусов этой страны, потому утвердился в умах олдфагов как православная программа для излечения всяческой заразы. Является произведением известного программиста Игоря Данилова. «Приходи ко мне лечиться и зайчонок, и волчица», — говорит И. Данилов. «И жучок, и паучок, и алкоголик-мужичок», — добавляет НОМ. Кстати, логотип компании Данилова как раз паучок, что, конечно же, символизирует.

Доктор Веб, как старейший антивирус, заслужил почитание у большинства олдфагов. Этим и примечателен. Был уличен в краже технологий AVP, правда, сразу же был оправдан. Весной 2005 по сети распространились слухи о слиянии двух крупнейших российских антивирусных компаний — «Лаборатории Касперского» и компании «Доктор Веб» (обратите внимание на дату). Позднее, весной 2009

года, слухи повторились вновь благодаря питательной почве затяжного мирового экономического кризиса. Теперь основным рефреном стала фраза: «Грусть, тоска? — купи ЛК!»

Само поделие отличается вполне вменяемыми методами работы, сравнительно малыми размерами дистрибутива и не убивающим моск интерфейсом. Есть версия под Линупс, да.

Есть бесплатная версия антивиря CureIt!, которая представляет собой Self-Extractor с урезанной по времени и возможности обновлять базы лицензией. Доставляет тем, что не требует ни денег, ни инсталляции. В системе после неё остаётся только .LOG. С недавних пор стала платной для коммерческого использования.

Алсо отметился наличием официального Live-CD, а впоследствии и Live-USB (Linux-based), на раз уничтожающего руткиты (не слишком стабильного поначалу, но чрезвычайно шустрого в сравнении с анальными поделками на основе Bart-PE). ВНЕЗАПНО также абсолютно бесплатен.

Также имеет Enterprise-версию, позволяющую ленивым одминам рулить сразу всеми установленными копиями в локалке, не отрывая задницу от любимого кресла.

Впрочем, есть мнение, что последние версии DrWeb жутко тормозят. 5.0 ещё можно терпеть, а вот 6.0 уже пытается соперничать с Каспером по этому показателю, инфа 100%. Кроме того, крайне геморройно удаляется из системы. Зачастую приходится прибегать к танцам, как и с поделками от Mail.ru.

Последняя версия имеет винрарную защиту от потери данных, поведенческий анализатор (HIPS) .

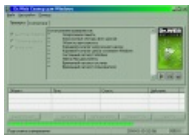
Служба поддержки по *nix-версиям часто отвечает на чистом bash'e или sed'e, что доставляет.

В стране бескрайних степей имеется свой офис «Центральная Азия», со своими лютыми манагерами, с хитрым планом по захвату компьютеров потребителей через AV-Desk. Отличается наличием собственной техподдержки и бесплатным трафиком для обновлений баз.

В DOS-эпоху антивирь имел текстовый файл с перечислением забавных вирусов и их действий, в основном перевирающих command.com ругательства, наподобие: «В вашем дисководе две дискеты».

Интересно, что баг в мобильной версии Dr.WEB, открывающий доступ в корень файловой системы, — единственное средство получения рута к смартфонам Nokia на Symbian 9 после прекращения их официальной поддержки.

Добрый доктор Данилов смотрит на Анонимуса, как на банку с малварью



Скромный доктор такой скромный

Avira

На славу постарались немцы, хотя и пересмотрели, судя по всему, фильмов про наемных киллеров. Как платная версия не стоит внимания. До поры была малоизвестна, на данный момент набирает популярность среди опытных юзверей.

Плюсы: не грузит систему, после установки ничего не просит и ничем не нагружает, неплохо локализована на русском. Минусы: с наемником не договориться, врагам — только пулю в лоб, лечить — а это как? — не удалять — вы что рехнулись? Ежедневная реклама, которая может вылезти во время игры и вызвать анальную боль у домашнего сундука. Самостоятельные ежедневные обновления вызывают баттхерт у обладателей мобайл-интернета с трафиком.

Касперский

Антивирус Касперского (он же *Свинья Касперского*, *Антивирус Каспийского*, *Анатолий Кашпировский*, *ЙаКасперско*, *Кошмарский*, *К. Спермский* и просто *Каспер*) — наиболее распиаренный антивирус, который постепенно захватывает весь мир и даже Северную Корею. Печально прославился тем, что старые его версии тормозили слабые компьютеры получше многих вирусов. В настоящее время проблема решена, однако в памяти хомячков стереотип жив

Антивирус Касперского — лютый агрегат, наполненный свистелками и перделками чуть более, чем полностью, что скоро приведет к тому, что он станет отдельным государством в вашем компьютере, ну или, в крайнем случае, автономией. Благодаря непродуманному кодингу на начальных версиях прославился тем, что тормозит компьютер получше многих вирусов. Поправить реноме, даже используя лютый пиар, теперь уже сложно, ибо Анонимус не забывает и не прощает. Бытует мнение, что антивирус Касперского настолько суров, что на его день рождения вымирают все вирусы. Также тормоза происходят из-за того, что Касперский проверяет файлы не только при запуске, но и при доступе и изменении (режим проверки «Интеллектуальный» по умолчанию), когда проводник обращается к файлам, браузер скачивает файл, монтируется образ.

Был платным долгое время (кроме Virus Removal Tool — аналога CureIt!), что порождало острую необходимость нагуглить бесплатных ключей. У продвинутых пользователей проблем не возникало, школьникам же поиск часто доставлял баттхерта, ибо троянов можно наловить на год вперед. Самые продвинутые в курсе, что пробная версия обладает всем функционалом полной в течение месяца с момента пробной активации, а информация о лицензиях сносилась батником из нескольких строчек (при выключенной самозащите и выгруженном антивирусе), поэтому вместо регулярного гугления держат на винте триал-ресет, против которого ЛК не видит смысл бороться, так как всё равно самые продвинутые пользователи сбросят дату активации. (Для устаревших версий). Сейчас существует урезанная бесплатная версия, делая нищебродам радостне.

Алсо, прославился звуком свиньи, который можно найти практически в любой библиотеке звуков, например, тут или тут. Звук стал мемом потому, что издается Касперским ВНЕЗАПНО при обнаружении вируса и заставляет срать кирпичами 95% населения, которые не меняют настроек по умолчанию. Именно ему посвящено множество цитат на Башорге. В последних версиях заменен на какую-то унылую скрипку, но *(спойлер:* сам файл со звуком свиньи никуда не делся, а обитает в %путь до каспера%\Skin\sounds под именем infected_p.wav.*)*

Также Евгений Касперский и продукт его жизнедеятельности люто форсится государственными каналами зомбоящика. Пиар в правительстве подействовал, и ему дали госпремию (вместе со Смешариками). Самого Касперского пригласили в общественную палату РФ (вместе с Тиной Канделаки), что символизирует.

В последнее время Касперский решил стать русским аналогом Великого китайского фаерволла. Десятки и сотни сайтов и форумов попадают под определение фишинговых ежедневно, хотя на самом деле таковыми не являются. Ко всему прочему, Касперский со своими адептами усиленно настраивает баннерорезки, но зачастую безграмотно. Подобные нападки на заработок веб-мастеров заставляют последних генерировать сотни НЕНАВИСТИ в секунду. Так что выкладывание свежих ключиков на своих варезниках хоть и слегка портит копирастические настроения Касперского, но на самом деле бьёт по владельцам многочисленных сайтов ещё сильнее.

Касперский утверждал, что Linux и Mac открыты для хакерских атак. ЧСХ, оказался близок к правде.

Также Касперский люто, бешено форсит идею тотального контроля всего интернета. Но при этом сделал публичное заявление в своей небыдловеской манере о великой пользе и необходимости торрентов и халявы для общества, чем окончательно спалился. По мнению пациента, контроль тырнета должен включать следующие пункты: лишение пользователей анонимности, введение интернет-паспортов (на владение которыми нужно сдавать экзамен), введение интернет-полиции для слежки за пользователями, отключение от интернета стран, которые не соблюдают эти пункты (sic!).

Сам же Касперский эпично соснул хуйцов именно из-за того, что его сын пренебрёг анонимностью и выложил все личные данные на себя ВКонтакте, которые и помогли его похитить. После похищения Касперский, ощутив баттхёрт, **поспешил написать письмо** о своей гениальной задумке самому Дурову.

С версии-2010 началось скатывание в сраное говно: сначала удалили из дефолтного скина активацию ключом (вернуть можно было, поставив сторонний скин), потом запустили процесс облондинивания скина (теперь место распределено нерационально, требуется много лишних кликов для выполнения повседневных задач), а затем и убрали из скина возможность его замены (сменить можно было, отключив самозащиту да подредактировав реестр). С выходом же версии-2014 хомячки, привыкшие крякать Каспера ключами, соснули хуйцов: возможность офлайн-активации ключом полностью выпилена.

Проактивная Защита полностью переделана и теперь работает самостоятельно под названием «Мониторинг активности», принимая все решения самостоятельно, не спрашивая у пользователя «А что делать с программой, которая перехватывает нажатия клавиш, может, запретить?», ведь Касперский лучше знает, что делать, сука!

Алсо Bloomberg обвинило лабораторию Касперского в связях с ФСБ аж с 2012 года, вызвав у Женьки лютый багет. Ответ был прост: это ваши домыслы, а крыса-кунов мы найдём и устроим им.

Свою порцию говна в вентилятор подбросил и Сноуден, из сливов которого следует, что американская гэбня на пару с британской долгое время внимательно следили за конторой Жени и выявили, что тот через этот свой антивирус ещё с 2008 тянет у своих клиентов как-то чересчур много лишних данных. Да так, что западным шпиёнам для того же самого и делать-то ничего не надо — достаточно просто перехватывать всё идущее на сервера Касперского и бережно складировать это у себя.

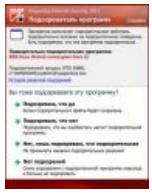
А в 2018-м Европка официально признала Каспер вредоносным ПО.

Но, как бы там ни было, вирусы он ловит довольно-таки неплохо. **См. также**

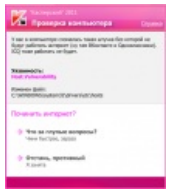
- Можно смотреть вечно на три вещи: как горят города, тонут люди и детектируются трояны
- Каспер в Абсурдопедии
- Касперский — 8-й из 15 самых опасных людей планеты

Бесплатный сыр

Ложное срабатывание



Пользователю приходится принимать подозрительно ответственные решения



Версия для гламурных кис

Продвинутый интерфейс такой продвинутый (Тёма причастен)

Типичный фанат поделия Касперского

Qihoo 360 Antivirus

Китай тоже не отстаёт от своих конкурентов и в 2009 году выходит на рынок со своим чудом 360 Total Security (позже переименовали). Ну как на рынок… Прога-то бесплатная…

Радует простотой интерфейса, маленькими системными требованиями, возможностями удалить Malware, пытающийся спиздить твой аккаунт (ИЧСХ, до этого лаборатория Касперского и Др. Веб не додумались, CureIt гарантирует это!), и даже чистить системный мусор! При этом ввиду отсутствия лишних свистоперделок не тормозит систему и самое себя. Один минус — у этого его QVM II много ложных срабатываний, но ведь ты знаешь, когда можно быть уверенным в том, что загружаешь/устанавливаешь, а когда лучше поостеречься, правда, пионер?

До поры до времени не имел мультиязычности, и пользователю оставалось «радоваться» китайскому интерфейсу, но где-то в 2013–2014 Qihoo поняли, что надо развиваться дальше Народной Республики, и создали WorldWide-версию со всеми языками, даже рюським!

В 2012 году вышли версии под Вёдра и Яблоки. Сюрприз, на китайском. Опять же спасла WW-версия. Может чистить оперативку и очищать мусор системы, уметь тасккиллер и даже находить смартфон по картам! Ламерьё утверждает: «Одна беда: на Linux это чудо так и не портировали…»

NOD32

NOD32 — антивирусный пакет, выпускаемый расово словацкой фирмой Eset. Название изначально расшифровывалось как Nemocnica na Okraji Disku — «Больница на краю диска» (перефразированное название популярного в Чехословакии телесериала «Больница на окраине города»). Впрочем, есть и другие трактовки.

NOD32 обеспечивает защиту компьютера от вирусов, троянов, а также от юзера методом его самоповешания. Как и любой коммерческий продукт, NOD32 провозглашается самым-самым крутым антивирусом во Вселенной. В подтверждение сего приводится аргумент, что весь код антивируса написан на языке ассемблера, что какбе намекае на быстродействие. Приобрел популярность у целевой аудитории из-за того, что совмещал два, казалось бы, несовместимых качества: он очень неплохо искал заразу и не грузил при этом систему.

Быдло тоже любит NOD, но совсем по другой причине: испокон веков процесс получения вечного триала очень толерантен к умственным способностям Анонимуса и варьируется от изменения одного значения в реестре (NOD 2.x) до запуска простенького батника (NOD 4) или же программы, которая сама будет лазить по сайтам с ключами и пихать их в Нод. А с появлением годовых ключей необходимость задействовать при активировании пакета церебральное утолщение нервной трубки у потребителя отпала и вовсе.

Так как NOD32 является одним из относительно новых на российском рынке антивирусов, а поклонников имеет много, он занял место генератора антивирус-холиваров. Практически на любом форуме можно найти тему «Касперский vs NOD32». Алсо, если есть тема типа «Доктор Веб vs Касперский», то фанаты НОДа обязательно устроят срач, а саму тему объявят ересью. То же самое не чуждо и фанатам Касперского. И так далее по кругу. И только самые тонкие тролли вовремя вспоминают про Symantec.

Кстати, если верить открытому письму сообщества, спионерившего в своё время с серверов ESET полный комплект IDA Pro 6, части исходного кода NOD32 в данный момент раскиданы по куче компьютеров, чьи владельцы скачали эту самую IDA. Исходники зашифрованы и инкапсулированы в архивы с дебаггером.

Нод и Башорг

- Оппа! Подозрительный файл передан в лабораторию для анализа.
- Теперь моя и без того маленькая комната завалена сотней коробок.
- Задолбали вы со своим Касперским, поставьте НОД, ОН ИХ НЕ ВИДЕТ!
- NOD32 от простуды.
- Че?

Нод нашёл Tibs по названию файла

Маскот Нода

Защищено даже от венеры! НОД гарантирует это!

Norton Antivirus

«Компьютерные вирусы — это такой же миф, как сказки о крокодилах, живущих в канализации Нью-Йорка. »

— Питер Нортон, 1988 г.

Norton Antivirus — антивирь от расово пиндосской фирмы Symantec. Сам Питер Нортон, написавший свой винрарный Коммандер, когда Женя и Игорёк ещё были студентотой, имеет весьма опосредованное отношение к антивирю (как, впрочем, и к Коммандеру). По крайней мере, большую популярность этот продукт получил после поглощения Peter Norton Computing Symantec'ом. Тем не менее, в своё время Norton был годным антивирусом, ещё в начале нулевых отлично работавшим на целеронах под Windows 98, которые Касперский намертво вешал. Затем антивирус где-то к 2005-й версии начал обрастать свистелками и перделками и постепенно скатился в сраное говно, по тормознутости заткнув практически всех конкурентов. Вдобавок, нынешние версии анально порабощают систему, и порой удаляется он исключительно вместе с виндой. Но вирусы ловит хорошо!

Microsoft Security Essentials

Microsoft Security Essentials — ВНЕЗАПНО антивирус от Microsoft. Быстрый, бесплатный, да ещё и вирусы ловит.
Когда-то давным-давно уже был продукт, называвшийся Microsoft Antivirus. Работал он под DOS, и это единственное, что о нём известно на сегодняшний день. Затем наступила эпоха рассадников вирусов, в середине нулевых MS одумалась и выкатила корпоративный Forefront, но настоящий butthurt у антивирусных компаний наступил с анонсом этого персонального антивиря. Фееричность ситуации заключается в том, что у MS непостижимым образом, путем покупки конторы Sybari[здесь должна быть штука про верёвочную обвязку *shibari*], получился кошерный продукт, хорошо ловящий вирусы, не тормозящий (кроме запущенных случаев типа Pentium III о 256 RAM), с нормальным интерфейсом. И бесплатный же! Но, разумеется, без ложки говна не обошлось: вместе с ним принудительно ставится средство проверки лицензионности винды, что мешает использовать его на ~95% Windows XP, установленных в этой стране и сопредельных государствах. Хотя правильно крякнутые висты и семёрки от него ничуть не страдают (при

наличии достаточно прямых рук пиратские XP не страдают также). В восьмерку и десятку прикручен сразу, правда, под псевдонимом Windows Defender. Для коммерческого использования есть вышеупомянутый MS Forefront. Бесплатный же Security Essentials, согласно лицензии, можно поставить на 10 ПК в фирме, правда, механизма проверки количества установок в сети и корпоративности этой сети в нём нет… ну ты понел. Можно подумать, что это хороший антивирь для дома, но как бы не так! Он создает лишь иллюзию защищенности и не защитит от zero day атак. Но что можно ожидать от бесплатного антивиря? Отсюда выходит, что нужен он только для отлова скачанных кряков и других спижженых плюшек.

Online

Вы почувствовали неладное после запуска кряка? Как-то комп стал притормаживать и вообще? Проверьте файл бесплатно онлайн сразу шестью десятками антивирусов.

Подобные сервисы также используются кулхацкерами для тестирования своих поделок на недетектируемость антивирусами. Однако тру-вирусописатели тестируют на закрытых сайтах, которые не отсылают сигнатурки в а/в компании.

Антивирь-срач

Хомячки готовы бесконечно доказывать крутость своего антивируса (особенно доставляет то, что большинство спорщиков, кроме своего, других пакетов собственно в глаза не видело). Срач давно вошел и прочно закрепился среди дисциплин специальной олимпиады. А так как объективной методики оценки антивируса до сих пор не придумали (результаты большинства синтетических тестов вроде VB100 показывают то, что хотели сказать спонсоры конкретного теста, и ничего больше), даже толстый тролль может росчерком пера вызвать многокилобайтный поток флуда.

На самом деле

В конечном итоге установка пользователем на домашний компьютер связки KAV/NOD32/Symantec/Dr.Web (нужное подчеркнуть) + Outpost Firewall (Norton Internet Security) являет собой лишь способ потешить своё ЧСВ, мол, вот какой я защищённый от внешних атак специалист.

Не стоит забывать еще о том, что антивирусы — это средство борьбы с неугодными программами. То есть, если по какой-то причине вы не понравились антивирусному вендору, весь ваш софт будет детектиться как малварный. За примерами ходить далеко не надо:

1. Windows Defender блокирует NoCD не потому, что там вирус, а потому что разработчики игры попросили MS внести этот файл в базу. Также Windows Defender был использован как средство борьбы с одной софтварной компанией. Чем спровоцировал олимпиаду «кто первым сломает новую версию PatchGuard» и статьи по взлому.
2. Антивирус навязывает вам способы писания программ и защиты их кода. Например, NOD, чтобы не заморачиваться с декриптовкой всевозможных пакеров и протекторов, просто заявил, что все, что упаковано, — все малварь. То есть шароварщики не имеют права использовать защиты, на которые у NOD’а нет анпакера, а писатели защит вообще сосут хуй — NOD блокирует даже закачки такого софта. Что об этом думают представители NOD’а, можно прочесть тут и тут

Антивирусы неиллюзорно доставляют тем, что рядовой юзер не понимает всего пиздеца происходящего. Представьте: у вас есть ОСь, хорошая и почти годная. И вот ОСь по каким-то причинам стала известной. Но операционка закрытая и исходников нет, поэтому вся забота о патчах ложится на владельцев исходного кода. Но ВНЕЗАПНО ваша скорость клепания патчей никого не устраивает, потому что дыры находятся быстрее, чем исправляются, и перед вами стоит выбор:

- Расшарить исходники в паблик и сделать операционку бесплатной и свободной для всех, после чего комьюнити допилит код довольно быстро;
- Нанять туеву хучу кодеров, которые ускорят выпуск патчей;
- Понаблюдать 5 лет за происходящим пиздецом, после чего нанять бригаду кодеров, которые положат болт на патчи и начнут клепать собственный антивирус с высокими потерями в производительности.

Угадайте, какой радужный путь был выбран.

Как страшно жить

Если вы все еще думаете, что ваш любимый антивирус защитит вас от напастей интернетов, то можете поставить для успокоения антивирус на обновление и дальше не читать. В реальности вы будете так думать до тех пор, пока на ваш комп не попадёт вирус или троян, который обойдёт антивирус. Для неисправимых параноиков у нас найдется пара дельных советов анальным рабам монопольной индустрии Мелкомягких

На одном небезызвестном форуме есть очень опытные аксакалы, которые путём долгой ебли мозгов себе и друг другу выработали политику анального огораживания NT-системы, настолько задротскую и эффективную, что она позволяет не только навсегда забыть об антивирусах, но даже пускать за компьютер школьников и представителей интеллектуальных большинств. Даже если вы целыми днями только и дрочите на прон-сайтах! Вот краткое изложение самых основных мер анального огораживания своей системы:

- Полная переустановка всей системы. Выделение системе отдельного логического диска, который не будет захламляться, для последующего ~~сноса системы~~ ускорения восстановления, дефрагментирования, бекапов и прочих нужностей.
- Отключение автозапуска на всех съёмных дисках — обязательно! Делается стандартной утилитой gpedit.msc, кому-то проще скачать AVZ4, но тру-одмины делают это через редактор групповой политики, либо вручную через regedit: очищают подразделы Run, RunOnce в кустах HKLM и HKCU, но это не защитит от двойного щелчка по значку флэшки с последующим срабатыванием авторана, для предотвращения чего нужно установить скрипт VirusVaccine для ленивых или же вручную в реестре прописать `"AutoRun"=dword:00000000` в ветке `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CDRom` и для особо хитрожопых программ `"*.*""=""` в ветке `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers\CancelAutoplay\Files`, так как в этой ветке программа ищет особые файлы, найдя которые не станет автоматически запускаться. Поэтому по умолчанию присваиваем значение «все файлы».
- Создание пользователя с ограниченными правами (если не в состоянии их настроить, ставьте права гостя). Следует учесть, что есть куча вирусной дребедени, прекрасно работающей с ограниченными правами (например, спиздить пароли очень легко, привилегии админа не требуются).
- Пользование кошерным браузером, запущенным из-под пользователя с ограниченными правами в Windows XP. Это делается из-под любого пользователя батником с одной строчкой. Например, из-под рута батником с содержимым runas /user:%название пользователя% /savecred «%ProgramFiles%\Opera\opera.exe»[1]. Ещё лучше — браузером с анально огороженными яваскриптами (под Лисой делается расширениями NoScript и uBlock Origin, под Хромом — расширением uBlock Origin, под Оперой — вот этим). Есть и минус — с отключёнными яваскриптами многие сайты работают не так, как хотелось бы. И вирусняк, пролезший через дырку в браузере, тоже будет работать с ограниченными правами. Систему не грохнет, но похулиганить в данной учётной записи может. В Windows 7/8/10 браузер можно запускать в админской учётке, включив UAC!
- Не запускать что попало, появившееся на компьютере. Если сильно жмёт, то для проверки появившегося как раз и используется антивирус — в этом случае он должен обновляться хотя бы раз в неделю и иметь включённый мониторинг файлов. Можно также политикой запретить исполняемые файлы (.exe).
- Иметь включенное автоматическое обновление критических апдейтов системы.
- Желательно также иметь нормально настроенный стандартный фаерволл.
- Запускать непроверенные программы внутри виртуалки.

Если же вы желаете уберечь себя от страшных и ужасных уязвимостей типа 0-day, вредоносного кода типа сассера, кидо и т. д., помогут следующие действия, при условии наличия домашнего компутера с интернетом и отсутствия Active Directory, средств разработки ПО, СУБД или еще каких-то специфических программ. После применения некоторых пунктов, особенно касающихся DCOM и отключения анонимного доступа к именованным каналам, проверить работоспособность специфических программ.

- При соблюдении условия повседневной работы под пользователем с ограниченными правами необходимо задать встроенному админу пароль позаковыристее.
- Отключите через services.msc и реестр вот этот список служб для повышения производительности системы.
- Для общего доступа к файлам и принтерам в настройках брандмауэра оставить только порт TCP 445 (если никому свои шары предоставлять не планируете, то закрывайте и этот порт, а в настройках сети на всех интерфейсах снимайте галки на «общем доступе к файлам и принтерам»)
- Отключить в диспетчере устройств драйвер NetBIOS over TCP/IP (Диспетчер устройств — Вид — Показать скрытые устройства — Драйверы устройств не Plug and Play — NetBIOS over TCP/IP — в Свойствах устанавливаем состояние «Отключено» и перезагружаемся). Стоит отметить, что далеко не во всех компьютерах стоит это делать, иначе просто после перезагрузки не выйдешь в интернеты.
- Через соответствующую оснастку запретите анонимный доступ к DCOM (\WINDOWS\system32\dcomcnfg.exe — Службы компонентов — Компьютеры — Мой компьютер — ПКМ — Свойства — Безопасность COM. Там же можно пройтись по отдельным компонентам системы).
- Разрешить политику «Сетевой доступ»: не разрешать перечисление учёток SAM и общих ресурсов анонимными пользователями (через gpedit.msc, раздел Конфигурация компьютера — Конфигурация Windows — Параметры безопасности — Локальные политики — Параметры безопасности).
- Настроить политику «Сетевой доступ»: Разрешать анонимный доступ к именованным каналам (открыть ее и удалить все, что там перечислено: COMNAP, COMNODE, SQL\QUERY, SPOOLSS, LLSRPC, browser), Разрешать анонимный доступ к общим ресурсам (открыть ее и удалить все, что там перечислено), Пути в реестре доступны через сетевое подключение (открыть ее и удалить все, что там перечислено).
- Установка игр и последующий запуск должны осуществляться не на реальную систему, а в так называемую песочницу. Не все программы согласны нормально работать в песочнице, и часто

грохаются (то есть завершают работу), но это как говорится, их проблемы. Кошерные проги BufferZone, Sandboxie, ZoneAlarm — друзья геймера-очкожима! (пользователи Windows XP Professional x64 Edition могут обломаться — ни одна из песочниц не работает).
- Стоит добавить также про относительно свежий метод борьбы — **DeepFreeze** aka «глубокая заморозка». Суть проста: состояние системного раздела зеркалится и автоматически возвращается к изначальному после перезагрузки, сметая с концами любые трояны, набранные за предыдущий сеанс работы. Но от кражи персональных данных не спасёт, если они есть на винчестере.

Как известно, настоящая компьютерная безопасность начинается с перерубленных проводов связи с внешним миром, закатывания компьютера в бетон и отправки его на орбиту. Всё остальное — полумеры, разве что переход в другое измерение спасёт гиганта мысли. Ну или установка x64 редакции XP/Vista/Win7, на которых имеется штатный kernel patch protection. Дополненная любым вшивым антивирусом, такая система окажется очень устойчивой.

См. также

- Антивирус Попова
- «Иммунитет»

Ссылки

- Свободный антивирус ClamWin
- Бесплатный антивирус для всех, да-да, и для барыг тоже
- Антивирусы на войне
- Антивирусы на войне 2 (Средневековье)
- Антивирусная трагедия (пьеса)
- Бесплатный антивирус Microsoft Security Essentials
- Для параноиков

Примечания

1. ↑ Здесь пользователя поджидает веселье с русской кодировкой

Software

12309 1C 3DS MAX 8-bit Ache666 Alt+F4 Android BonziBuddy BrainFuck BSOD C++ Chaos Constructions Cookies Copyright Ctrl+Alt+Del Denuvo DOS DRM Embrace, extend and extinguish FL Studio Flash FreeBSD GIMP GNU Emacs Google Google Earth I2P Internet Explorer Java Lolifox LovinGOD Low Orbit Ion Cannon Me MediaGet MenuetOS Microsoft Miranda Movie Maker MS Paint Open source Opera PowerPoint PunkBuster QIP Quit ReactOS Rm -rf SAP SecuROM Sheep.exe Skype StarForce Steam T9 Tor Vi Windows Windows 7 Windows Phone 7 Windows Phone 8 Windows Vista Wine Winlogon.exe Wishmaster Word ^H ^W Автоответчик Антивирус Ассемблер Баг Билл Гейтс и Стив Джобс Блокнот Бот Ботнет Браузер Варез Винлок Вирусная сцена Генерал Фейлор Глюк Гуй Даунгрейд Демосцена Джоэл Спольски Донат Защита от дурака Звонилка Интернеты Кевин Митник Китайские пингвины Костыль Красноглазики Леннарт Поттеринг Линуксоид Линус Торвальдс Лог Ман Машинный перевод Мегапиксель

w:Антивирус en.w:Antivirus