

# Автор: Георгий Курячий

## Вредоносное программное обеспечение

С лёгкой памяти "лихих 90-х", времени ДОСа, гибких дисков и компьютерных вирусов, заставляющих буквы падать, всевозможные вредоносные программы нередко называют просто "вирусами". Хуже того, сочное, запоминающееся слово "вирус" рождает в уме неискушённого пользователя совершенно фантастические представления о том, что такое "вредоносное ПО" и как от него уберечься. Здесь мы попытаемся бегло обрисовать настоящее положение дел с вредоносным ПО, чтобы методы защиты от него в области СПО были достаточно очевидны.

## Инструментарий компьютерного хулигана -- заботы самого хулигана

Оговоримся сразу, что в наш обзор не будут входить программные продукты, используемые компьютерными взломщиками, хакерами и прочими персонажами, с деятельностью которого связывается в народе слово "вирус". В самом деле, даже самый асоциальный компьютерный взломщик может пользоваться вполне законными программными продуктами -- компилятором, отладчиком, сетевым инструментарием -- для своих тёмных делишек. Даже специальные программы для взлома, т. н. rootkits, хотя и представляют серьёзную опасность для взламываемого компьютера, не могут особенно интересовать добропорядочного пользователя. Общим для всех этих (не рассматриваемых далее) программных продуктов является то, что запускаются они *с ведома пользователя*. Это значит, что пользователь, запускающий такую программу сам прекрасно представляет её вредоносные свойства, а следовательно, он и есть злоумышленник, что переводит обзор в административную и моральную плоскости.

## Корень зла

Итак, общим для всего рассматриваемого класса вредоносного ПО является способность производить не прошенные пользователем, таинственные, а потому -- ужасные действия. Говоря формально, *потенциально* вредоносным является ПО, возможности которого не до конца документированы. Злоумышленник (или программа, написанная злоумышленником) может втайне от пользователя воспользоваться недокументированной возможностью ("проэксплуатировать" её), и здесь только от воли злоумышленника зависит, насколько результаты этой "эксплуатации" будут в самом деле вредоносными.

Это открывает один курьёзный угол рассмотрения проблемы. По сути потенциально вредоносным является любое, самое обычное, программное обеспечение -- операционная система или прикладное ПО, -- если в него (намеренно или по недосмотру) заложены недокументированные возможности. Тогда собственно "вирусы" -- продукт жизнедеятельности злоумышленника -- вторичны по отношению к этому ПО, они возникают как бы сами собой, в ответ на "провокацию" -- заманчивую возможность эксплуатации системы.

Так или иначе, эти "продукты жизнедеятельности" -- это программы (и только программы), "паразитирующие" на теле не вполне здоровых ОС или программного продукта, о существовании которых пользователь не подозревает до тех пор, пока их действия не станут очевидными. Здесь аналогия с вирусом достаточно полная: имеется факт заражения -- установка вредоносной программы в систему, как и в случае настоящего вируса, не замечаемая вирусом-носителем, инкубационный период, в течение которого работа вируса не заметна и симптомы болезни, отражающие активную работу этой программы.

## Что такое "вирус"...

Итак, "вирус" -- это программа (и только программа). Это совсем не означает, что вирус -- это "файл с расширением .exe". Программы встречаются внутри операционной системы и программных продуктов в разных обликах. Помимо собственно исполняемых файлов (к которым стоит причислить в случае Windows ещё довольно большое множество файлов, включая даже шрифтовые), программа может быть частью другой программы, которую она модифицировала (довольно типичное поведение ДОСовских вирусов 90-х), может представляться модулем или сценарием для определённого ПО (популярный пример -- макровирусы для программы Microsoft Word), может, наконец, вписывать себя в разнообразные хранилища данных, которые не являются программами, но части которых в определённых условиях выполняются как программы (пример -- т. н. загрузочные вирусы, поражающие загрузочную область жесткого диска, данные из которой загружаются и выполняются до загрузки операционной системы).

Поскольку вирус -- это программа, само наличие его на каком-либо устройстве хранения данных ещё не означает "заражённости компьютера" в данный момент. Вирус (программу) надо сначала *запустить* -- непосредственно, либо запустив заражённую им программу. Именно работающая вредоносная программа причиняет вред. Кстати, если программа уже загружена, поздно предпринимать какие-то меры против неё, так как, "первой встав", она может предотвратить попытки себя обезвредить. Так, известны вредоносные программы для Windows, устанавливающиеся на равных правах с драйверами устройств и контролирующими тем самым любой доступ к дискам или памяти; они отслеживают большинство известных антивирусов и способны обмануть их, либо нарушить их работу.

## ... и с чем его едят?

Проблема первоначального запуска решается вирусом множеством различных способов. Если он уже активен в системе, к его услугам и подсистема автоматического запуска служб, и модификация имеющихся. Если вирус неактивен, он может стать активным при участии пользователя, но без его ведома. Например, в системах семейства Windows практикуется т. н. автозапуск программ с носителя: когда ОС определяет, что подключен новый носитель данных, она ищет на этом носителе файл специального формата (`autorun.inf`) и выполняет все команды, в нём записанные. Вирусу остаётся только модифицировать этот файл. Автозапуск на флеш-дисках -- очень частая причина заражения вредоносной программой.

Другой вариант -- обмануть пользователя, выдав программу за обновление системы, а то и просто за картинку, которая внезапно запускается как программа (используются различные недокументированные возможности файловых навигаторов, почтовых программ и т.п.).

Очень большое значение в распространении вредоносного ПО имеет *обмен* программами и документами, которые могут содержать автоматически выполняемые вредоносные сценарии. Если пользователю по какой-то причине *захотелось* такой документ открыть, или запустить полученную программу, дело злоумышленника в шляпе.

На пересечении обмана и обмена лежат всевозможные сайты, содержащие контрафактное ПО (часто уже заражённое). Несоответствие информации, видимой пользователем, допустим, в окне WWW-навигатора, и информации, которую этот навигатор на самом деле обрабатывает, даёт злоумышленникам дополнительные возможности. Не следует забывать, что современные WWW-навигаторы имеют свойство автоматически выполнять на компьютере пользователя части программ, скачиваемых с web-сайта. Активные элементы, написанные на javascript, имеются на подавляющем большинстве сайтов, но помимо javascript есть ещё java-апплеты, Flash-ролики и некоторые другие инструменты. Ошибка или недосмотр в каждом таком "исполнителе" может привести к запуску вредоносной программы.

Огромное количество вредоносного ПО распространяется с электронной почтой, тому причина -- слабые ограничения почтового протокола и множественные недосмотры в популярном почтовом ПО для ОС Windows.

## Как вылечить грипп?

Довольно распространённым является заблуждение, что если "в файле обнаружен вирус", этот файл можно "вылечить". На самом деле таким свойством обладали только "настоящие вирусы" -- ДОСовские файловые вирусы, а из более современных -- макровирусы в документах. На сегодня в подавляющем большинстве случаев речь идёт о заражении *системы*, а не файла. Это значит, что для "излечения вируса" необходимо удалить вредоносное ПО и отменить сделанные им изменения в системе. Последняя задача -- самая сложная, и далеко не всегда выполнимая.

Словом, лечить надо не грипп, а человека. Проверка почтовой переписки и *удаление* писем, содержащих вредоносное ПО практически никогда (или вовсе никогда -- один шанс из миллиона) не вредит переписке. То же относится к фильтрации доступа к файловым архивам и некоторым другим превентивным мерам. Если некий файл нельзя получить, потому что он "содержит вирус", этого делать и не надо, потому что ничего, кроме вредоносного ПО, в этом файле и нет.

Такая вредоносная программа называется обычно "троянской" или "spyware" -- в зависимости от того, какие функции выполняет и каким способом была получена и активизирована на компьютере. Оба термина, как и термины "backdoor", "червь" и другие, достаточно размыты и представляют интерес только классификаторам вредоносного ПО и просто интересующимся этой темой.

## Cui prodest?

Такая картина (саморассылающееся по почте вредоносное ПО без примеси какой-бы то ни было полезной нагрузки для пользователя) резко контрастирует с картиной, имевшей место лет десять-пятнадцать назад. Во времена "ДОСовских вирусов" практически каждый экземпляр вредоносного ПО "цеплялся" за какой-нибудь полезный исполняемый файл, а антивирус "лечил" этот файл, уничтожая вирус и восстанавливая нормальную работу программы.

В написании таких вирусов даже усматривалась особая хакерская "дисциплина": поражённая программа должна вести себя как здоровая (за исключением активизации собственно вируса), вирус не должен заражать сам себя, он должен уметь "убегать" от антивируса и т. п. Какие вредоносные действия будет совершать вирус, автору было совершенно неважно: это могли быть весёлые шутки, вроде экрана кверху ногами, осыпающихся букв или песенки "чижик-пыжик" (которую наигрывал... дисковод!), а могли быть и необратимые деструктивные действия, вроде удаления информации с жёсткого диска и даже порчи содержимого ППЗУ определённого типа (знаменитые "Сih" и "Чернобыль").

Однако времена молодецкой удали прошли. Сегодня вредоносное ПО -- это в первую очередь (а возможно -- и во все остальные) **бизнес**.

Какую прибыль может получить от эксплуатации чужого компьютера? Ответ очевиден: воспользоваться ресурсами этого компьютера:

1. Вычислительная мощность. Например, можно заставить подбирать пароль к ещё не взломанной учётной записи
2. Дисковое пространство. Разместить на компьютере склад контрафактного ПО, аудио- и видеоматериалов, и прочего содержимого, которое легально распространять нельзя.
3. Учётные записи. Учётные записи пользователя можно использовать для доступа к различным ресурсам как в локальной сети, так и в сети Интернет. Особенный интерес представляют средства электронного платежа: номера кредитных карт и т. п.
4. Сетевые ресурсы. Эта составляющая используется наиболее активно, в основном за счёт массовых рассылок.
5. Мозг пользователя. Несмотря на угрожающую формулировку, эта категория вредоносного ПО довольно курьёзна: можно, например, заставить пользователя решать CAPTCHA для интересующих злоумышленника сайтов.

Самый прибыльный на сегодня бизнес такого рода -- массовая рассылка непрошенной почты, т. е. спама. Не имея возможности рассылать её с собственных серверов, давно и прочно занесённых во всевозможные "чёрные списки", новоявленные "почтальоны" прибегают к жёстким вирусным технологиям. Каждый пользовательский компьютер, заражённый спам-агентом ("ботом") становится источником рассылки как непрошенной почты, так и экземпляров таких же и других ботов. Конгломерат из многих тысяч заражённых компьютеров (т. е. "ботнет") управляется централизованно с серверов компании-злоумышленника.

Среди ботнетов нет места какой-либо дисциплине, кроме диктата прибыли. Заражённый компьютер продолжает работать более или менее сносно только до тех пор, пока с него можно рассылать спам. Дальнейшее хозяев ботнета не интересует. Зачастую никакое лечение такого компьютера невозможно и требуется полное удаление данных и переустановка системы.

## Вирусы и Linux

Прежде, чем перейти к советам касательно защиты от вредоносного ПО в Linux, заметим, что ситуация с вредоносным ПО в мире свободного ПО вообще и Linux в частности *значительно* отличается от таковой в области несвободного ПО.

**Распространение вредоносного ПО под Linux не имеет эпидемического характера.**

Причин тому несколько.

Первая и главная причина состоит в том, что пользователю *дистрибутива* Linux крайне редко выпадает необходимость устанавливать стороннее, непроверенное ПО. В дистрибутив входят тысячи программных продуктов, в соответствующем хранилище (репозитории) их находится ещё больше. Огромный выбор проверенного и централизованно распространяемого свободного ПО, для получения которого нет необходимости ни во взломе, ни в подборе регистрационной информации, делает ситуацию "скачал с одного хакерского сайта дистрибутив, с другого -- ломалку, запустил сначала одно, потом другое" совершенно нетипичной. Под Linux существуют и несвободные программы -- например, игровое или специализированное ПО, но и эти программы нередко можно бесплатно скачать с сайта *производителя* (как, например, Skype или Adobe Acrobat Reader, в этом случае производитель гарантирует отсутствие вредоносности). Платные несвободные программы, такие, как игры, всё чаще распространяются по гибридной схеме: "движок" скачивается бесплатно, а "начинку" -- игровые уровни и прочее -- можно купить в составе игры для Windows.

1. Не последнюю роль играет также строгое разделение прав пользователей. В Linux только один пользователь -- т. н. "суперпользователь" -- имеет право произвольно модифицировать операционную систему: менять настройки, устанавливать и удалять ПО, исправлять системные файлы и т. п. "Обычный" пользователь Linux в принципе не может изменить настройки операционной системы. Не могут этого сделать и отдельные сетевые службы, каждая из которых запускается с правами какого-либо "обычного" пользователя, к тому же дополнительно поражённого в правах. Значимые системные службы, которым требуются суперпользовательские права, зачастую запускаются в т. н. изолированном окружении (chroot), что не позволяет им модифицировать настройки вне этого окружения. Заметим, что даже здесь речь идёт о *потенциальном* взломе ОС, а не о каких-то действительных угрозах. Наконец, администратору компьютера категорически не рекомендуется постоянно работать в режиме суперпользователя, достаточно выполнять в таком режиме только выбранные команды. Например, для администрирования персонального компьютера достаточно, по большому счёту, двух действий, требующих суперпользовательских прав:

1. установки и удаления ПО (посредством обращения к надёжному хранилищу)
2. настройки сетевого подключения

2. Для свободного ПО в целом не стоит проблема всеобщей совместимости исполняемых форматов. Это значит, что готовый программный продукт, собранный, допустим, для дистрибутива ALT Linux, совершенно не обязан работать в составе дистрибутива Gentoo Linux. Свободный программный продукт всегда доступен в исходных текстах на языке программирования, и сообщество любого Linux-дистрибутива предпочтёт изготовить *свою собственную* версию исполняемой программы, со своими, присущими только этому сообществу модификациями. Результат, с точки зрения пользователя, будет примерно одинаковым: программный продукт будет выполнять все возложенные на него функции. А вот с "точки зрения вируса" ситуация станет просто ужасной: все программы, даже ядро операционной системы, *внутри себя* совершенно разные, даже в рамках разных версий одного и того же дистрибутива. Найдя способ проэксплуатировать одну конкретную уязвимость одной конкретной программы злоумышленник откроет себе "лазейку" на компьютеры только с установленной *определённой версией определённого дистрибутива Linux...* до первого обновления!

3. Стоит сказать пару слов об оперативности исправления ошибок, в том числе ошибок, связанных с безопасностью. Свободное ПО подразумевает беспрепятственный доступ к исходным текстам. Это означает, что над поиском ошибок в свободной программе работает, считай, всё прогрессивное человечество. Злоумышленнику найти такую ошибку, разумеется, также проще, чем найти ошибку в программе без исходных текстов. Но что ему сделать намного сложнее, чем в случае несвободного ПО, так это успеть проэксплуатировать эту ошибку *раньше*, чем она будет обнаружена и *исправлена* свободным сообществом. В свободном ПО существует традиционная практика исправлять ошибки, связанные с безопасностью, *до того*, как информация об этих ошибках станет достоянием общественности. Задержка между обнаружением ошибки и её исправлением в составе хранилища составляет несколько *часов*, в то время как ошибки в несвободных продуктах могут "висеть" неисправленными по месяцу. Хитрость в том, что тот, кто обнаружил ошибку в свободной программе, может тут же её исправить!

4. Наконец, не стоит забывать, что Linux-системы не обрели столь массового распространения, чтобы наличие одной общей уязвимости вызывало эффект эпидемии.

Считается, что большинство взломов Linux происходит либо вручную, непосредственно злоумышленниками, либо путём последовательного применения всех известных вредоносных инструментов, позволяющих проэксплуатировать ту или иную уязвимость в прикладном ПО определённой версии. Такую активность (например, определённого вида запросы HTTP-серверу) сравнительно легко отследить в системном журнале, как администратору, так специально обученному "сторожу" (например, с помощью Snort). Тем самым предотвращается даже *потенциальная* возможность атаки на компьютер, независимо от того, может ли вообще она быть успешной.

## Что делать?

Правила гигиены при работе с Linux очень похожи на общие правила поведения за компьютером. Однако по Linux их намного проще соблюсти!

1. Не скачивать и не устанавливать подозрительного ПО.
2. Не изменять настройки системы с правами суперпользователя и вообще не работать с такими правами, если вы до конца не знаете, что именно делаете.
3. При обнаружении ошибки сообщать о ней сообществу через систему отслеживания ошибок. Вам скажут спасибо: тем самым вы поможете не только себе, но и всем остальным пользователям.
4. Отслеживать обновления системы на предмет безопасности.
5. Содержать в чистоте и порядке свои учётные записи, не пользоваться ненадёжными паролями и не хранить пароли в доступном кому бы то ни было месте. Особенно это относится к паролю суперпользователя!