Профилактика заражения «флешки» компьютерным вирусом

Сначала кратко. Чтобы обезопасить свою флешку от вредоносного программного обеспечения (ПО) выполните два действия:

1. Создайте в её корневом каталоге папку с именем `autorun.inf`
2. Поместите в эту папку какой-нибудь файл

Разумеется, этот способ вовсе не панацея от инфицирования, но многие из вирусов вполне благополучно сдержать может. Ниже будет рассказано, как именно предлагаемый способ работает, а так как я ни разу не системный администратор, то излагать буду в меру своего понимания, поэтому должен заранее извиниться за возможные технические неточности.

Начать следует с того, что в операционных системах (ОС) семейства Windows предусмотрена возможность некоторых действий, сопутствующих подключению носителя информации. Так, например, при вставке в привод CD-ROM компакт-диска на нём можно разместить инструкции автоматического запуска небольшой программы, облегчающей работу с содержимым этого диска. Сами инструкции записываются в корневом каталоге носителя в виде обычного текстового файла с именем “autorun.inf”*.

Реальность такова, что многие придумки, нацеленные на что-то хорошее (в том числе – на удобство и простоту), начинают использоваться в дурных целях. Эта печальная участь постигла и автозапуск, так как он стал применяться для распространения вредоносного ПО. Способ инфицирования компьютера так называемым авторан-вирусом очень прост: вы вставляете заражённую флешку в USB-порт, ОС её подключает и сканирует у неё корневой каталог на наличие файла “autorun.inf”, после чего выполняет команды в нём, нисколько не интересуясь вашим мнением, ведь чаще всего в настройках ОС автозапуск не отключен. В содержимом файла “autorun.inf” вполне достаточно одной команды – на запуск также обычно присутствующего в корневом каталоге флешки файла с расширением “exe” (то есть файла исполняемого, проще говоря – программы), который и является «телом» вируса. Стартовав, вирус заражает компьютер и среди прочего заботится о своём дальнейшем размножении: теперь при подключении иного флеш-накопителя он в его корневом каталоге запишет свою копию (исполняемый файл) и “autorun.inf”, также содержащий инструкцию запуска себя любимого. Чтобы пользователь ничего не заметил, оба эти файла будут иметь атрибут «скрытый», ведь мало кто настраивает штатный «Проводник» (или какой иной используемый файловый менеджер) на отображение скрытых файлов. По итогу вы будете иметь ещё одну завирусованную флешку.

Не каждый знает, что папка (синонимы – каталог, директория) на самом деле представляет из себя файл, только особый, так как содержит в себе ссылки на другие файлы (места их расположения на носителе), которые для нас, пользователей, обычно визуализируются «Проводником» как находящиеся внутри этой папки. Многие из нас также привыкли, что удаление каталога с файлами внутри не вызывает никаких затруднений, хотя на самом деле в ОС существует запрет на стирание папки (особого файла), содержащей хотя бы один файл (то есть хотя бы одну ссылку на другой файл). Дело в том, что при попытке уничтожить непустую папку ОС на самом деле сначала очищает её содержимое, а уж только потом удалению подвергается и сама директория.

В свете сказанного становится понятным, как описанный в самом начале настоящей заметки способ помогает уберечься от «цифровой инфекции». Если на флеш-накопителе уже будет непустая папка “autorun.inf”, то при подключении его к заражённому компьютеру

---

* Статья “Autorun.inf” // RU.WIKIPEDIA.ORG: Википедия. Свободная энциклопедия..
URL: https://ru.wikipedia.org/wiki/Autorun.inf (дата обращения: 15.02.2023)

обосновавшийся на нём вирус просто будет не в силах эту папку переписать, заменив обычным текстовым файлом, хотя, вероятно, своё «тело» (exe-файл) в «корне» флешки и оставит, однако оно будет невидимым (скрытым) и запускать его придётся уже вручную, предварительно обнаружив – сомневаюсь, что найдётся много желающих это сделать, нормальный пользователь подобные находки предпочитает сразу удалять от греха подальше.

Думаю, стоит повториться: предлагаемый метод не даёт 100%-ой гарантии безопасности, меры по её обеспечению должны быть комплексными: имеет смысл на своём компьютере отключить автозапуск (как это сделать – легко нагуглить), установить антивирусную программу и поддерживать её базы данных в актуальном состоянии.

Возможна организация ещё одной дополнительной линии обороны, правда в наши дни, к сожалению, малоактуальной, так как из-за желания сэкономить, упростив и удешевив производство, многие изготовители флеш-накопителей ныне выпускают свою продукцию без специального механического переключателя, позволяющего физически заблокировать возможность записи на устройство. А зря – весьма типична ситуация, когда нужно собственную флешку подключить к незнакомому компьютеру, дабы просто «скинуть» с неё информацию и предварительная блокировка записи давала бы уверенность, что вы потом не притащите на свою домашнюю или рабочую машину пакостный «подарочек». Мне, кстати, однажды довольно забавно было наблюдать, как заражённый компьютер соответствующими сообщениями начал настойчиво умолять снять защиту от записи, когда я в него воткнул «заблоченную» флешку – вирус, видать, чувствовал, гад, что вот-вот его прихлопнут, ведь на той флешке был антивирусник записан, готовый к бою без всякой инсталляции.