Е. А. Королькова

ИССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ ВИРУСОВ И ИХ ВЛИЯНИЕ НА БЕЗОПАСНОСТЬ ДАННЫХ

В настоящее время информационные технологии развиваются стремительными темпами. По этой причине, все больше и больше появляется компьютерных вирусов. В данной статье представим определение компьютерному вирусу и рассмотрим их виды, взаимодействие с файлами, а также все возможные способы защиты и предотвращения заражения системы.

Введение

Персональные компьютеры пользователей все чаще становятся жертвами вредоносных программ. В результате заражения появляется риск утечки различных персональных данных: от логинов и паролей, до данных банковских карт. Для борьбы с угрозами необходимо иметь максимально полное и актуальное представление о разнообразии вирусов, а также об их воздействии на атакуемую систему.

Основная часть

Компьютерный вирус – это программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но, и могут кардинально отличаться. В настоящее время известно более 5 тыс. программных вирусов, которые можно классифицировать по следующим признакам:

- среда обитания
- способ заражения среды обитания
- воздействие
- особенности алгоритма

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные. Сетевые вирусы распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули, то есть в файлы, имеющие расширения EXE и COM. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и теряют способность к размножению. Загрузочные вирусы внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска. Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков. По способу заражения вирусы делятся на резидентные и нерезидентные. Резидентный вирус при заражении компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время. По степени воздействия компьютерные вирусы можно разделить на следующие виды:

- неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах
- опасные вирусы, которые могут привести к различным нарушениям в работе компьютера
- очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия. Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Можно отметить вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии. Известны вирусы-невидимки, называемые стелс-вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Наиболее трудно обнаружить вирусы-мутанты, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Имеются и так называемые квазивирусные или «троянские» программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков. Основными путями проникновения вирусов в компьютер являются съемные диски, flash

- накопители, а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с источника, содержащего вирус.. Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус, прежде всего, переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, становится возможным заражение других файлов. При заражении компьютера вирусом важно его своевременно обнаружить. Для этого следует знать основные признаки проявления вирусов. К ним можно отнести:

- прекращение работы или неправильная работа ранее успешно функционировавших программ
- прекращение работы или неправильная работа ранее успешно функционировавших программ
- неожиданное значительное увеличение количества файлов на диске
- медленная работа компьютера
- невозможность загрузки операционной системы
- изменение даты и времени модификации файлов
- изменение размеров файлов
- подача непредусмотренных звуковых сигналов

Вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Главное помнить, что вирусы важно обнаружить на раннем этапе их развития, когда еще не все файлы были повреждены. Чтобы раньше обнаружить и избавиться от них, необходимо регулярно выполнять проверку антивирусными программами. Пренебрежение проверок может привести к плачевным последствиям, что не только ваш компьютер будет заражен, но и другие. Поэтому стоит разобраться какие типы антивирусов существуют:

- Антивирусы детекторы. Их принцип работы – это сообщать пользователю, что вирус обнаружен.
- Антивирусы ревизоры запоминают начальное состояние программ, файлов, чтобы в дальнейшей своей работе сравнивать с текущим.
- Фильтры выявляют подозрительные процедуры, отслеживают изменения программ, файлов, дисков. Данные антивирусы следят, например, изменялся ли размер файлов. При обнаружении каких-то подозрительных действий фильтры запрашивают пользователя о правомерности их выполнения.
- Доктора самый распространённый тип. Такие антивирусы помимо обнаружения вирусов, могут от них и избавиться.
- Антивирусы Вакцины. Они изменяют программы, файлы таким образом, что для вирусов они уже выглядят зараженными.

Антивирусы не способны обнаружить любой вирус. Ведь это программа способна найти и избавиться только от известных ей вредоносных файлов. Для конкретного вируса пишется антивирус только, если программист будет иметь хотя бы один экземпляр вредоносного кода. Если не делать ничего для защиты, то последствия заражения могут быть очень серьезными.

Заключение

На сегодняшний день написано множество различных вирусов, но и безопасность не стоит на месте, ежедневно развиваясь для успешного противодействия стоящим угрозам. Создаются новые и совершенствуются имеющиеся антивирусные программы. Вместе с тем как мы уже выяснили, многое зависит не только от программ - антивирусов, но и от цифровой гигиены самого пользователя электронного устройства.

1. Безруков Н.Н. "Классификация компьютерных вирусов MS-DOS и методы защиты от них Москва, СП "ICE 1990 г.
2. Безруков Н.Н. "Компьютерные вирусы Москва, Наука, 1991.
3. Денисов Т.В. "Антивирусная защита"//Мой Компьютер-№4-1999г.
4. Мостовой Д.Ю. "Современные технологии борьбы с вирусами"// Мир ПК. - №8. - 1993.
5. Ф.Файтс, П.Джонстон, М.Кратц "Компьютерный вирус: проблемы и прогноз Москва, "Мир 1993 г.
6. Зенкин Д. В., Касперский Е. В. Компьютерные вирусы: происхождение, реальная угроза и методы защиты
7. Каптерев А.И. Электронный учебник по информатике

Королькова Екатерина Алексеевна, студент 1 курса факультета информационной безопасности Белорусского государственного университета информатики и радиоэлекстроники, ek2352290@gmail.com

Научный руководитель: Кукин Дмитрий Петрович, заведующий кафедры вычислительных методов и программирования Белорусского государственного университета, кандидат технических наук, доцент, kukin@bsuir.by.