Современные технологии, несмотря на долгий путь развития, еще молоды, но всѐ же виртуальная реальность – это следующий большой рывок в развитии сферы образования. И в ближайшее время есть возможность увидеть множество интересных открытий в этой области.

УДК 372

Пашковский В. И.

РАЗНОВИДНОСТИ КОМПЬЮТЕРНЫХ ВИРУСОВ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ. ОСНОВНЫЕ АНТИВИРУСНЫЕ ПРОГРАММЫ

БНТУ, г. Минск
Научный руководитель: доктор техн. наук, доцент Азаров С. М.

В 1961 году инженеры Виктор Высоцкий, Дуг Макилрой и Роберт Моррис из фирмы Bell Telephone Laboratories разработали маленькие программы, способные делать копии самих себя. Это были первые вирусы. Они были созданы в виде игры, которую инженеры назвали «Дарвин», целью которой было отправлять эти программы друзьям, чтобы посмотреть, какая из них уничтожит больше программ оппонента и сделает больше собственных копий. Игрок, которому удавалось заполнить компьютеры других, объявлялся победителем.

Вирусами их назвали по аналогии с биологическими вирусами, вызывающими болезни. Чтобы размножаться обычному вирусу необходим живой организм, в котором он будет создавать свои копии, так и компьютерному вирусу для существования необходима своя среда для размножения.

Вирус – это вредоносная программа. Из определения мы можем понять одно: вирус – это программа. Значит, подобно всем другим программам на вашим компьютере она будет храниться в двоичном формате в одном из этих мест:

Жесткий диск или SSD диск.

Жесткий диск компьютера напоминает огромную библиотеку с кучей книг (ваших файлов и программ), закодированных в двоичном формате (0 и 1). Эти книги будут лежать на своих полочках до тех пор пока вы не захотите их сжечь или выкинуть (удалить). Даже если вы выключите компьютер вся информация на нѐм останется.

Оперативная память.

Принцип работы этой памяти достаточно прост, она варьируется, как только вы нажали включения компьютера и тут же пошли записи всех посещенных вами мест, папок на ПК, можете иногда заметить что при первом открытии папки или файла это занимает некоторое время, а при повторном нажатии папка открывается моментально, ну или на порядок быстрее, потому что это действие было временно сохранено на оперативную память. Поэтому чем больше объем такой памяти, тем лучше. Но как только вы выключили компьютер, временная память очищается безвозвратно. В ней как правило хранятся самые сложные полиморфные вирусы.

Сегодня все современные вирусы создаются злоумышленниками, имеющими цель заполучить конфиденциальные данные пользователя или использовать его компьютер в личных целях.

Компьютерные вирусы – это проблема с которой сталкивался любой пользователь компьютера. Чем больше мы пользуемся компьютером, тем больше неприятностей мы испытываем из-за заражения вирусами. В данной статье мы рассмотрим основные виды компьютерных вирусов. Компьютерные вирусы делят на несколько типов, в зависимости от их вредоносной деятельности.

Червь – программа, которая делает копии самой себя. Ее вред заключается в захламлении компьютера, из-за чего он начинает работать медленнее. Отличительной особенностью червя является то, что он не может стать частью другой безвредной программы в отличии от файлового вируса.

Файловые вирусы – очень старый вид компьютерных вирусов. Задача файлового вируса заражать все исполняемые файлы, тем самым распространяясь и заражая новые компьютеры. Как правило, такие вирусы просто размножаются и разрушают операционную систему. Сейчас данный вид компьютерных вирусов теряет популярность. Вирусописатели предпочитают писать вирусы, которые приносят им доход.

Трояны или троянские программы это вредоносные программы, разработанные для кражи информации с компьютера жертвы. Логины, пароли, банковская и личная информация, большинство троянских программ воруют все что можно и отправляют эту информацию своему разработчику. Под видом троянских программ можно считать.

Кей-логеры (шпионы). Данные программы записывают все нажатия клавиш и действия пользователя за компьютером. После этого все собранная информация отправляется разработчику вируса. Таким образом, могут быть украдены пароли и другие важные данные, которые пользователь не сохранял на компьютере.

Вирусы-маскировщики – Rootkit.

Эти вирусы используются для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Rootkit'ы также могут модифицировать операционную систему на компьютере и заменять основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

Бэкдоры – вид компьютерных вирусов, который также можно считать подвидом троянов. Задача бэкдора поставить компьютер жертвы под контроль разработчика вируса. В случае заражения бэкдором вирусописатель может не только воровать данные, но и управлять компьютером.

Боты – еще один представитель семейства троянов, более продвинутый тип бэкдора. Установившись на компьютер бот, с помощью интернета вступает в контакт с разработчиком и другими зараженными компьютерами, создавая, таким образом, огромную компьютерную сеть. Такие сети называют бот-нетами. При этом разработчик вируса получает под свой контроль не один компьютер, а сотни и тысячи компьютеров входящих в такую сеть. Подобные бот-неты могут использоваться для рассылки спама, DDoS атак, установки на компьютеры жертвы майнинг машин или распространения других вирусов.

Adware – вредоносное программное обеспечение, разработанное для демонстрации рекламы. Данный вид компьютерных вирусов после проникновения на компьютер начинает демонстрировать жертве различную рекламу.

Блокираторы – данный вид компьютерных вирусов блокирует операционную систему, отдельные ее функции или шифрует файлы на компьютере. После чего вирус начинает вымогать. Как правило при невыполнении определѐнных условий (чаще всего это перевод денег на кошелёк вымогателя) блокиратор удаляет все файлы жертвы с компьютера.

Теперь, основываясь на этих знаниях, можно заняться защитой от вирусов, троянских и других вредоносных программ. Основным средством борьбы с вирусами были и остаются антивирусные программы. Для того чтобы антивирусные программы эффективно выполняли свои функции, необходимо строго соблюдать рекомендации по их применению, описанные в документации. Особое внимание следует обратить на необходимость регулярного обновления вирусных баз данных и программных компонент антивирусов. Современные антивирусы умеют загружать файлы обновлений через Интернет или по локальной сети. Однако для этого их необходимо настроить соответствующим образом.

Однако даже без применения антивирусных программ можно постараться предотвратить проникновение вирусов в компьютер и уменьшить вред, который они нанесут в случае заражения. Вот что следует для этого сделать в первую очередь:

– блокируйте возможные каналы проникновения вирусов: не подключайте компьютер к Интернету и локальной сети компании, если в этом нет необходимости, отключите устройства внешней памяти, такие как дисководы.

– изготовьте системную загрузочную дискету, записав на нее антивирусы и другие системные утилиты для работы с диском, а также диск аварийного восстановления Microsoft Windows;

– проверяйте все программы и файлы документов, записываемые на компьютер, а также дискеты с помощью антивирусных программ новейших версий;

– устанавливайте программное обеспечение только с лицензионных компакт-дисков;

– ограничьте обмен программами и файлами;

– регулярно выполняйте резервное копирование данных;

– устанавливайте минимально необходимые права доступа к каталогам файлового сервера, защищайте от записи каталоги дистрибутивов и программных файлов;

– составьте инструкцию для пользователей по антивирусной защите, описав в ней правила использования антивирусов, правила работы с файлами и электронной почтой, а также опишите действия, которые следует предпринять при обнаружении вирусов.