ВРЕДОНОСНЫЕ ПРОГРАММЫ И ИХ КЛАССИФИКАЦИЯ. ОСНОВНЫЕ КАНАЛЫ РАСПРОСТРАНЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ И ДРУГИХ ВРЕДОНОСНЫХ ПРОГРАММ.

Трофимович А.В.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Существует класс программ, которые были изначально написаны с целью уничтожения данных на чужом компьютере, похищения чужой информации, несанкционированного использования чужих ресурсов и т. п., или же приобрели такие свойства вследствие каких-либо причин. Такие программы несут вредоносную нагрузку и соответственно называются вредоносными. **Вредоносная программа** – это программа, наносящая какой-либо вред компьютеру, на котором она запускается или другим компьютерам в сети.К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Для распространения вредоносные программы используют следующие объекты и каналы:

- файлы исполняемых программ;
- файлы офисных документов;
- файлы интерпретируемых программ;
- загрузочные секторы дисков и дискет;
- сообщения электронной почты;
- пиринговые (файлообменные) сети;
- интрасеть или Интернет;
- драйверы ОС;
- флеш-накопители.

Вредоносные программы делят на три подкатегории: *вирусы и черви*, *троянские программы* и *вредоносные утилиты*.

Компьютерный вирус – это программа, способная создавать свои дубликаты и внедрять их в вычислительные сети и файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению. Условно жизненный цикл любого компьютерного вируса можно разделить на пять стадий:

- проникновение на чужой компьютер;

- активация;
- поиск объектов для заражения;
- подготовка копий;
- внедрение копий.

Вирусы делятся на загрузочныеи файловые вирусы. *Загрузочный вирус* заражает загрузочный сектор винчестера или дискеты и загружается каждый раз при начальной загрузке операционной системы. *Файловый вирус* записывает свой код в тело программного файла или офисного документа. При этом во время запуска программы вирус получает управление.

Червь (сетевой червь) – это вредоносная программа, распространяющаяся по сетевым каналам, которая способна к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий. Жизненный цикл червей состоит из следующих стадий:

- проникновение в систему;
- активация;
- поиск объектов для заражения;
- подготовка копий;
- распространение копий.

В зависимости от способа проникновения в систему черви делятся на типы:

- *Сетевые черви*, которые для своего распространения используют локальные сети и Интернет;
- *Почтовые черви*, которые распространяются с помощью почтовых программ;
- *IM-черви*, которыеиспользуют системы мгновенного обмена сообщениями;
- *IRC-черви***,** распространяющиеся по каналам IRC;
- *P2P-черви***,** распространяющиеся при помощи пиринговых файлообменных сетей.

Троянская программа– вредоносная программа, используемая злоумышленником для сбора информации, её разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях. В отличие от компьютерных вирусов и червей троянские программы неспособны к самовоспроизведению. Жизненный цикл троянов состоит всего из трех стадий:

- проникновение в систему;
- активация;

- выполнение вредоносных действий.

Троянские программы классифицируются в соответствии с типом действий, выполняемых ими на компьютере. Троянская программа *бэкдор*предоставляет злоумышленникам возможность удалённого управления заражёнными компьютерами. *Эксплойты*– это программы с данными или кодом, использующие уязвимость в работающих на компьютере приложениях. *Руткиты*– это программы, предназначенные для сокрытия в системе определённых объектов или действий. *Банковские троянцы* предназначены для кражи учётных данных систем интернет-банкинга, систем электронных платежей и кредитных или дебетовых карт. *ПрограммыTrojan-Downloader* способны загружать и устанавливать на компьютер-жертву новые версии вредоносных программ, включая троянские и рекламные программы. *Игровые троянцы* крадут информацию об учётных записях участников сетевых игр. *Программы Trojan-IM* крадут логины и пароли к программам мгновенного обмена сообщениями. Также встречаются другие виды троянских программ.

Вредоносные утилиты– это вредоносные программы, предназначенные для автоматизации создания вирусов, червей или троянских программ. Подкласс вредоносных утилит делится на поведения в соответствии с совершаемыми действиями. *Программы-конструкторы* предназначены для создания новых вирусов, червей и троянских программ. *DoS*– осуществляют атаки типа «отказ в обслуживании» на компьютер-жертву.*Email-Flooder* используют для того, чтобы переполнить каналы электронной почты бессмысленными сообщениями.

Таким образом, исходя из всего выше перечисленного, можно сделать вывод, что вирусы и вредоносные программы способны наносить значительный ущерб, реализуя любые угрозы информации – угрозы нарушения целостности, конфиденциальности, доступности. Поэтому сегодня очень важно защищать компьютеры при помощи установления и обновления антивирусных программ.