Лекция
по дисциплине «Программно-аппаратная защита информации»

на тему: «Вредоносное программное обеспечение»

Вопросы:

- Определение и виды вредоносного ПО

- Компьютерные вирусы
- Охранный софт
- Критические точки системы

Определение вредоносного ПО

Вредоносные программы (malware , сокращение от malicious software) – общее название для всех программ и приложений, целью которых заведомо является нанесение того или иного вреда конечному пользователю.

Классы malware чрезвычайно многочисленны и разнообразны, однако в целом по характеру поведения и распространения все антивирусные компании подразделяют их на три главных рода – троянские кони (Trojan), черви (Worm) и классические вирусы (Virus).

Trojan – отдельное приложение, распространяемое разнообразными способами: по электронной почте, через сети обмена файлами, посредством интернет-пейджеров и так далее.

Цель программ этого рода – хищение информации, вымогание денег за восстановление предварительно зашифрованных пользовательских данных и тому подобные действия, направленные на получение выгоды, чаще всего финансовой.

Существуют даже коммерческие троянцы, с документацией и технической поддержкой. В настоящее время это самый популярный род вредоносных программ в Сети.

Worm – также отдельное приложение, распространяемое разнообразными способами: по электронной почте, через сети обмена файлами, посредством интернет-пейджеров, через уязвимости системы и так далее.

Способ распространения у них такой же, как и у троянцев. Отличие состоит в поведении: черви направлены не на воровство данных, а на нанесение вреда системе. Главным образом это реализуется либо удалением системных файлов, либо модификацией повреждением реестра, что делает систему неработоспособной.

Virus – самый старый род вредоносных программ, классические вирусы.

Эти программы изменяют исполняемые файлы, то есть «заражают» их, дописывая в них свой (вредоносный) код. Как следствие, каждый раз при исполнении зараженного файла выполняется код вируса. Сейчас количество программ этого рода значительно уменьшилось, однако они попрежнему представляют угрозу: для антивируса род Virus наиболее сложен в лечении.

Кроме того, существует род группы риска (RiskWare) и прочих вредоносных программ. Это не очень многочисленная группа программ, которые не выполняют непосредственно вредоносных действий, но потенциально опасны. Сюда относят рекламные программы (AdWare), программы-шутки (Hoax), хакерские инструменты (SpamTool, VirTool) и некоторые другие.

Отдельной группой следуют:

BackDoor – вредоносная программа, предоставляющая злоумышленнику удаленный доступ к зараженному компьютеру. После установки в систему бэкдор либо ожидает входящих соединений от хозяина, либо сам пытается с ним соединиться.

RootKit – программа, перехватывающая и изменяющая системные функции с целью скрытия или маскировки файлов, процессов, ключей реестра и так далее.

Также следует упомянуть достаточно растяжимое понятие «шпион» (Spyware) - программа, осуществляющая шпионаж того или иного рода.

Malware использует различные способы проникновения на компьютер пользователя:

- Вирус можно занести на дискете, диске, Flash-брелке и так далее. Некоторые вирусы копируют себя на сменные диски и заражают каждый компьютер, в который вставят такой диск.
- Вирус можно получить по электронной почте в качестве вложения в письмо.
- Вирус можно получить, перейдя по ссылке или посетив сайт.
- Вирус можно получить, устанавливая полезную программу – с компакт-диска или скачанную из Интернета.
- Вирус можно просто получить, если выйти в сеть без защиты.

Незащищенный компьютер в сети остается чистым в среднем 20 минут.

Компьютерные вирусы

Компьютерный вирус — это своеобразное явление, возникшее в процессе развития компьютерной техники и ИТ.

Суть его состоит в том, что программы-вирусы обладают свойствами, присущими живым организмам, они рождаются, размножаются и умирают.

Термин «компьютерный вирус» впервые употребил сотрудник Университета Южной Калифорнии Фред Коэн в 1984 г. на 7-й конференции по безопасности информации, проходившей в США. Этим термином был назван вредоносный фрагмент программного кода.

Компьютерные вирусы способны делать практически то же, что и настоящие вирусы: переходить с одного объекта на другой, изменять способы атаки и мутировать.

Проникнув, компьютерный вирус может ограничиться безобидными визуальными или звуковыми эффектами, но может и вызвать потерю или искажение данных, утечку личной и конфиденциальной информации. В худшем случае, КС пораженная вирусом, окажется под полным контролем злоумышленника.

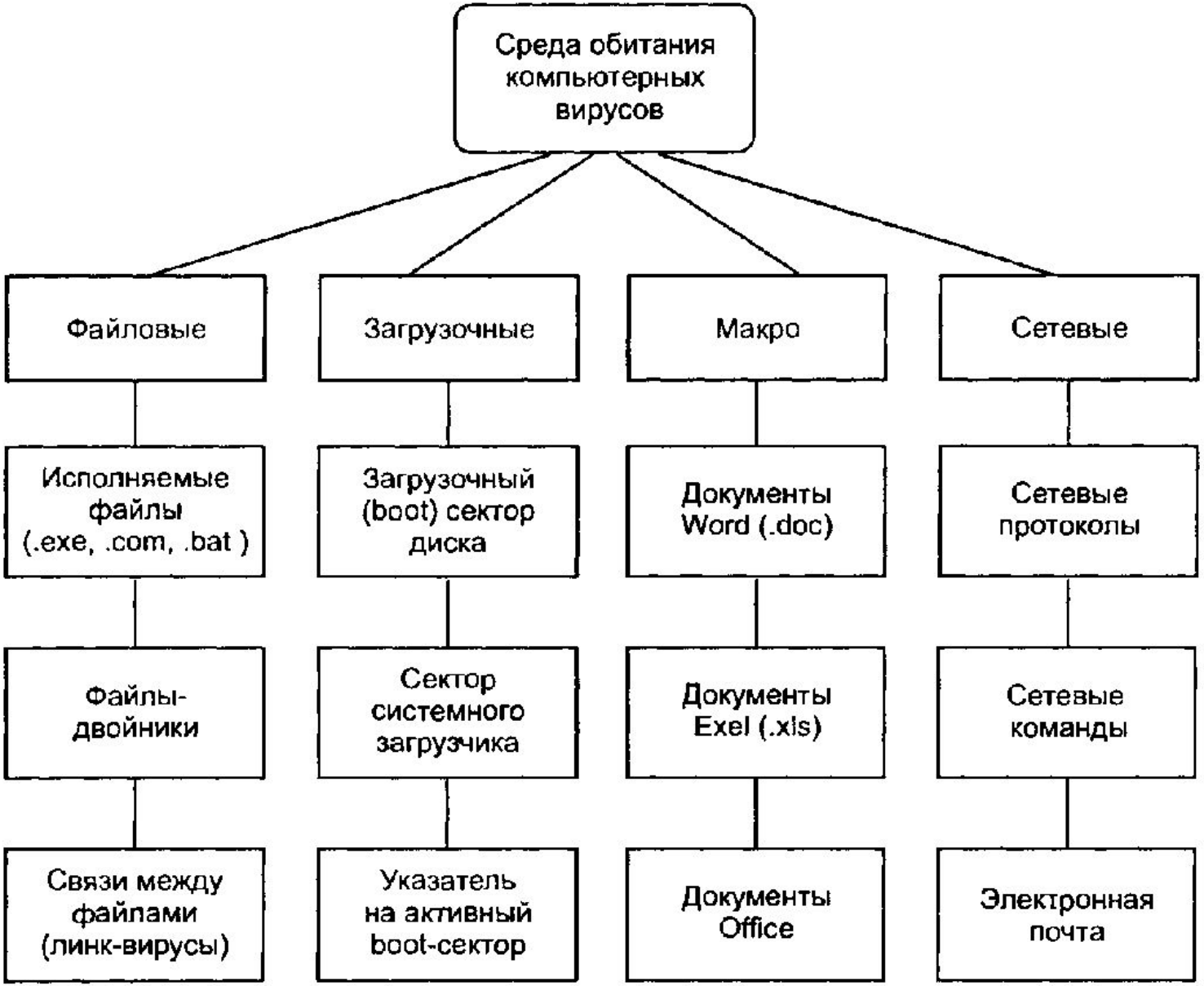
В настоящее время под компьютерным вирусом принято понимать программный код, обладающий следующими свойствами:

- способностью к созданию собственных копий, не обязательно совпадающих с оригиналом, но обладающих свойствами оригинала (самовоспроизведение);
- наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.

Вирусы можно разделить на классы:

- по среде обитания;
- операционной системе (ОС);
- особенностям алгоритма работы;
- деструктивным возможностям.

Основной и наиболее распространенной классификацией компьютерных вирусов является классификация *по среде обитания*, или *по типам объектов* компьютерной системы, в которые внедряются вирусы.


Среда обитания компьютерных вирусов
Файловые
Загрузочные
Макро
Сетевые
Исполняемые файлы (.exe, .com, .bat)
Загрузочный (boot) сектор диска
Документы Word (.doc)
Сетевые протоколы
Файлы-двойники
Сектор системного загрузчика
Документы Exel (.xls)
Сетевые команды
Связи между файлами (линк-вирусы)
Указатель на активный boot-сектор
Документы Office
Электронная почта

Файловые вирусы либо внедряются в выполняемые файлы (наиболее распространенный тип вирусов) различными способами, либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record). Загрузочные вирусы замещают код программы, получающей управление при загрузке системы. В результате при перезагрузке управление передается вирусу. При этом оригинальный boot-сектор обычно переносится в какой-либо другой сектор диска. Иногда загрузочные вирусы называют *бутовыми вирусами*.

Макровирусы заражают макропрограммы и файлы документов современных систем обработки информации: документы и электронные таблицы популярных редакторов Microsoft Word, Microsoft Excel и др. Для размножения макровирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла в другие. Вирусы этого типа получают управление при открытии зараженного файла и инфицируют файлы.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существуют также смешанные типы, которые совмещают в себе сразу несколько технологий.

Охранный софт

Антивирус – это программа, использующая специальную обновляемую базу данных для детектирования вредоносных программ. С этой целью используются так называемые сигнатуры, добавляемые в базу вирусными аналитиками компании.

Сигнатура содержит фрагмент кода вредоносной программы, который сравнивается со сканируемыми файлами; если сигнатура совпадает, файл признается зараженным.

Основные составляющие любого антивируса – файловый и почтовый сканер по доступу (on-access), иначе называемый монитором, сканер по требованию (on-demand), карантин и модуль обновления баз.

Ряд антивирусов использует так называемый веб-сканер – анализатор содержимого веб-страниц.

Антишпион – это инструмент поиска известных шпионских модулей по различным признакам. Как правило, антишпион оснащен сканером по требованию и некоторым количеством специализированных настроек системы или вспомогательных инструментов. Некоторые из них имеют полноценный или частичный монитор и самозащиту.

Антишпионы проигрывают любому антивирусу, однако они могут быть полезны при устранении последствий, главным образом – в исправлении системного реестра.

Host Intrusion Prevention Systems (HIPS), или средства предотвращения вторжений локального базирования - это системы анализа и блокировки опасных системных функций. В отличие от антивирусов, системы HIPS не имеют сигнатур и не детектируют вирусы – они позволяют управлять разрешениями на совершение определенных действий со стороны приложения.

Эффективность HIPS чрезвычайно высока и может доходить до 100% при блокировании любых вирусов, как известных, так и неизвестных, однако большинство таких систем требуют высокой квалификации пользователя. Существует несколько видов HIPS – классические, экспертные HIPS и HIPS на основе технологии Sandbox.

Классические HIPS – это системы, оснащенные открытой таблицей правил. На основании такой таблицы драйверы HIPS разрешают /запрещают определенные действия со стороны приложений либо спрашивают пользователя, что следует предпринять. Такие системы не пользуются популярностью у непрофессионалов, так как очень часто задают вопросы, что раздражает пользователя.

Экспертные HIPS называют еще поведенческими эвристиками. На основании анализа действий приложения HIPS этого типа выносят вердикты о его вредоносности.

HIPS типа Sandbox построены на принципе минимального взаимодействия с пользователем. В основе песочницы – принцип разделения приложений на доверенные и недоверенные.

Вопросы?