Методы и средства защиты компьютерной информации

Лекции 7-8.

Компьютерные вирусы.

Основы антивирусологии

Определение компьютерного вируса

Компьютерным вирусом называется программа (некоторая совокупность исполняемого кода и данных), которая обладает способностью создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты и ресурсы компьютерных систем, сетей и т.д. без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.

Фред Коэн, 1983

История компьютерных вирусов. Основные этапы.

- **«Доисторический»** (70-80 гг)
  - Первые теоретические труды
  - Вирусы-легенды
  - Возникающие инциденты
- **«До-интернетовский»** (80-90 гг)
  - Появление первых вирусов
  - Классические вирусы MS-DOS
- **Интернет-этап** (90-2000 гг)
  - Черви
  - Трояны
- **Современный этап** (2000 - современность)
  - Криминализация
  - Использование интернета в преступных целях

Причины возникновения вирусов

- Компьютерное хулиганство
  - Группа 1: Студенты и школьники
  - Группа 2: «Профессионалы»
  - Группа 3: Исследователи
- Мелкое воровство
- Криминальный бизнес
  - Обслуживание спам-бизнеса
  - DdoS-атаки
  - Отсылка платных sms-сообщений
  - Воровство интернет-денег
- Полулегальный бизнес
  - Принудительная реклама
  - Порно-бизнес, платные Web-ресурсы

Три условия существования вредоносных программ

- **Популярность** - широкое распространение и известность данной системы
- **Документированность** - наличие разнообразной и достаточно полной документации по системе
- **Незащищенность** системы или существование известных уязвимостей в ее безопасности и приложениях

Способы проникновения вредоносных программ в систему

- **Социальная инженерия** - тем или иным способом заставляют пользователя запустить заражённый файл или открыть ссылку на заражённый веб-сайт

- **Технические приемы внедрения** - осуществляется это через уязвимости в системе безопасности операционных систем и в программном обеспечении. Наличие уязвимостей позволяет изготовленному злоумышленником сетевому червю или троянской программе проникнуть в компьютер-жертву и самостоятельно запустить себя на исполнение без ведома пользователя

- **Одновременное использование социальной инженерии и технических методов**

Классификация вредоносных программ

- **Вирусы и черви** - вредоносные программы, которые обладают способностью к несанкционированному пользователем саморазмножению в компьютерах или компьютерных сетях, при этом полученные копии также обладают этой возможностью.
- **Троянские программы** - вредоносные программы, которые созданы для осуществления несанкционированных пользователем действий, направленных на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей
- **Вредоносные утилиты** - программы, разработанные для автоматизации создания других вирусов, червей или троянских программ, организации DoS-атак на удаленные сервера, взлома других компьютеров и т.п.

Правила именования вредоносных программ

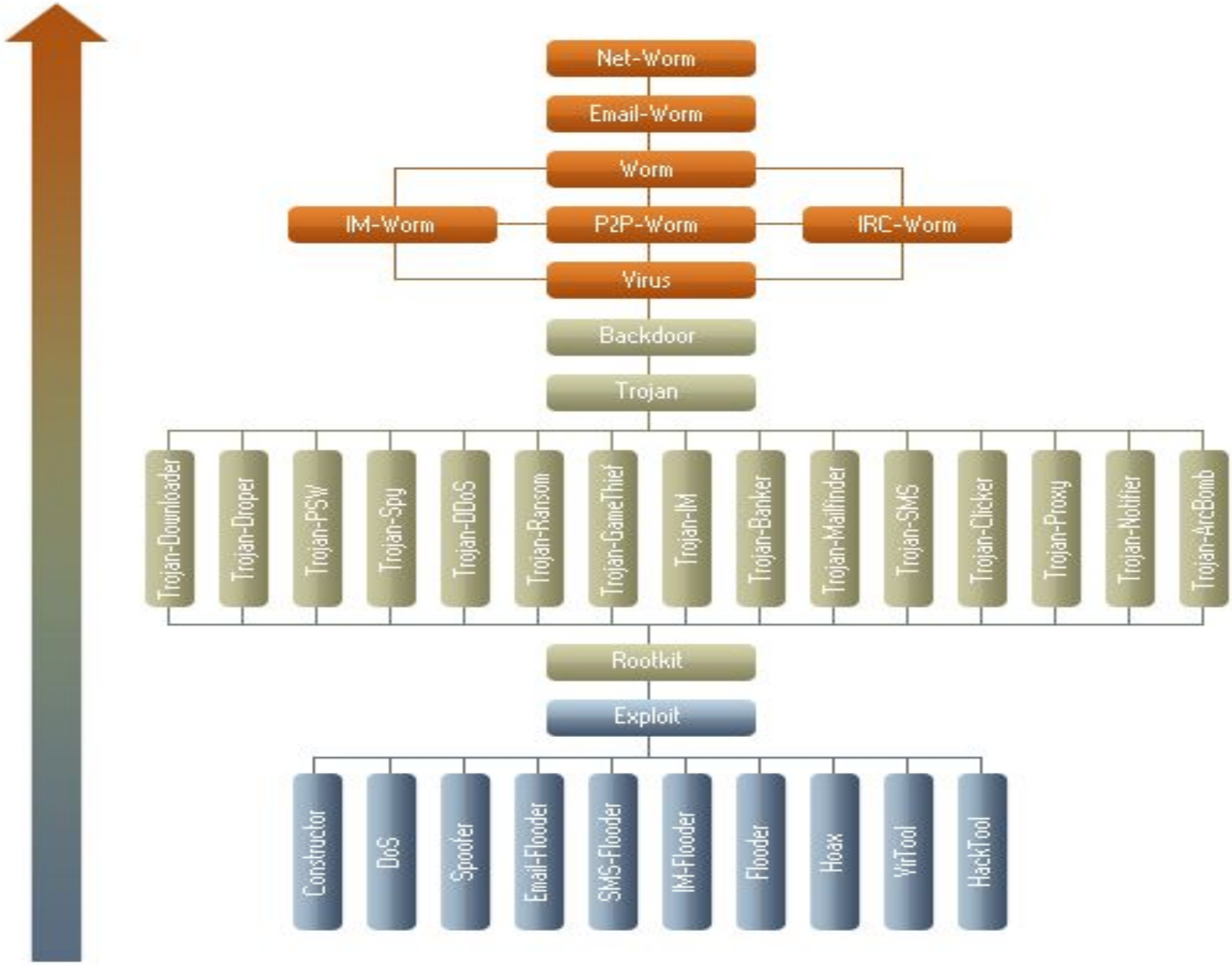
Behavior.Platform.Name[.Variant]

Behavior — определяет поведение детектируемого объекта. Для вирусов и червей поведение определяется по способу распространения; для троянских программ и вредоносных утилит — по совершаемым ими действиям; для PUPs — по функциональному назначению детектируемого объекта.

Platform — среда, в которой выполняется вредоносный или потенциально-нежелательный программный код. Может быть как программной, так и аппаратной. Для мультиплатформенных детектируемых объектов используется платформа с названием Multi.

Name — имя детектируемого объекта, позволяет выделять семейства детектируемых объектов.

Variant — модификация детектируемого объекта. Может содержать как цифровое обозначение версии программы, так и буквенное обозначение, начиная с «a»: «a» — «z», «aa» — «zz», ...


Net-Worm
Email-Worm
Worm
IM-Worm
P2P-Worm
IRC-Worm
Virus
Backdoor
Trojan
Trojan-Downloader
Trojan-Dropper
Trojan-PSW
Trojan-Spy
Trojan-DDoS
Trojan-Ransom
Trojan-GameThief
Trojan-IM
Trojan-Banker
Trojan-MailFinder
Trojan-SMS
Trojan-Clicker
Trojan-Proxy
Trojan-Notifier
Trojan-ArcBomb
Rootkit
Exploit
Constructor
DoS
Spoofer
Email-Flooder
SMS-Flooder
IM-Flooder
Flooder
Hoax
VirTool
HackTool

Классификация компьютерных вирусов

- **По среде обитания вируса**
  - Файловые вирусы
  - Загрузочные вирусы
  - Сетевые вирусы
  - Макро вирусы
  - Flash-вирусы
- **По способу заражения**
  - Резидентные вирусы
  - Нерезидентные вирусы
- **По деструктивным возможностям**
  - Безвредные
  - Нарушение работоспособности компьютера
  - Потеря или кража информации
  - Отказ работы «железа»

Особенности современных вирусов и алгоритмов их работы

- **Stealth** (стелс, невидимость) – способность вируса заражать файлы скрытно, не давая пользователю повода заподозрить неладное
- **Polymorph** (полиморфизм) – способность вируса шифровать свое тело так, чтобы никакие две копии вируса не были похожи друг на друга
- **Armored** (защита, бронирование) – способность вируса сопротивляться отладке и дизассемблированию
- **Multipartite** (многосторонность) – способность вируса заражать и программы, и загрузочные сектора дисков

Правовые аспекты. Статья 272 УК РФ

Неправомерный доступ к компьютерной информации

- Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.
- То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Правовые аспекты. Статья 273 УК РФ

Создание, использование и распространение вредоносных программ для ЭВМ

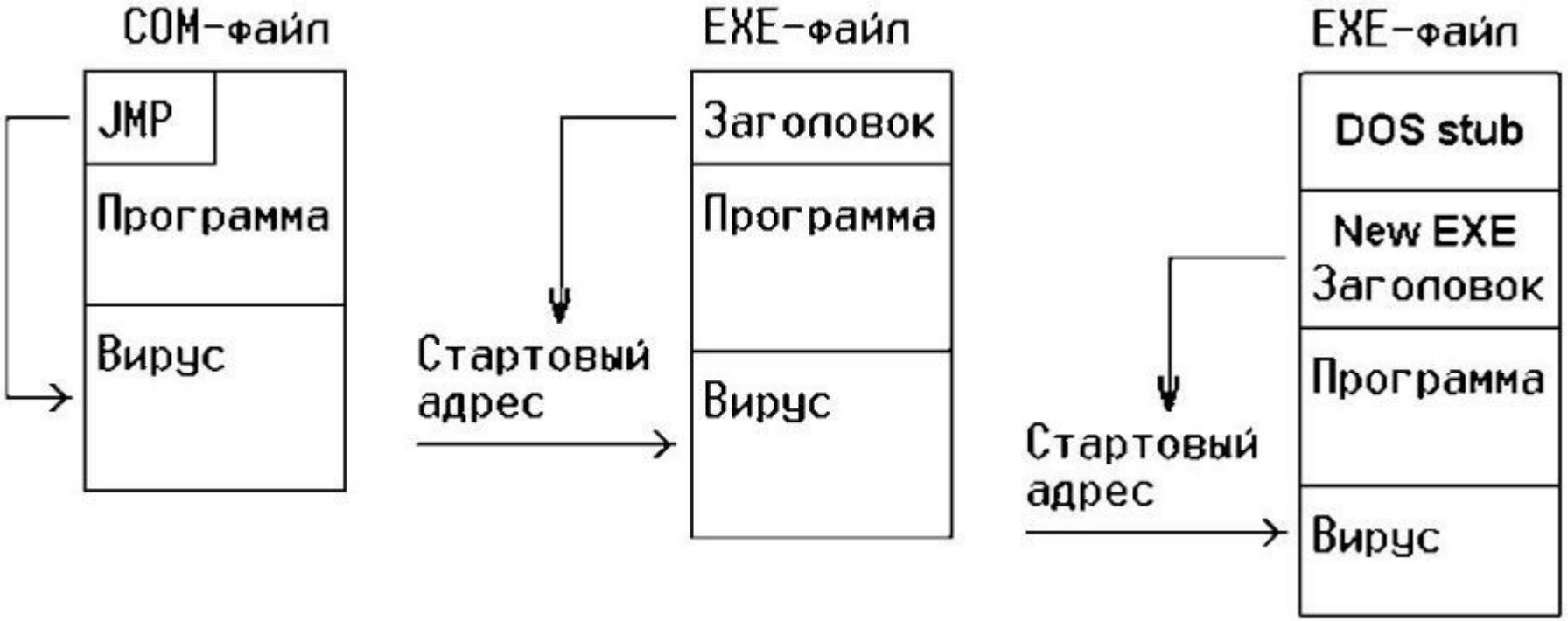
- Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами- наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.
- Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Правовые аспекты. Статья 274 УК РФ

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

- Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред,- наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.
- То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.

Работа файлового вируса



Загрузка и выполнение COM-программы

- Запускаемой программе отводится вся свободная в данный момент ОП. Сегментная часть начального адреса этой памяти обычно называется начальным сегментом программы.
- По нулевому смещению в сегменте, определяемом начальным сегментом программы, EXEC строит специальную служебную структуру PSP (Program Segment Prefix), в котором содержится информация,необходимая для правильной работы программы . Заполняет PSP операционная система (ОС), а его размер всегда равен 100h (256) байт .
- Сразу вслед за PSP загружается сама COM - программа
- EXEC выполняет настройку регистров процессора:
  - CS = DS = SS = ES указывают на начальный сегмент программы,
  - регистр IP инициализируется числом 100h
  - регистр SP инициализируется числом 0fffeh .
- Теперь загруженную COM - программу можно исполнить . Для этого EXEC передает управление по адресу CS : 100h.

Работа вируса в зараженной программе

- Восстанавливает в памяти компьютера исходные три байта зараженной программы
- Ищет на диске подходящий COM - файл
- Записывает свое тело в конец этого файла
- Заменяет первые три байта заражаемой программы командой перехода на свой код, сохранив предварительно исходные три байта в своей области данных
- Выполняет вредные действия, предусмотренные автором
- Передает управление зараженной программе . Поскольку в COM - файле точка входа всегда равна CS : 100h, можно не выполнять сложных расчетов, а просто выполнить переход на этот адрес

Параметры антивирусов

- **Надежность и удобство работы** — отсутствие «зависаний» антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.
- **Качество обнаружения вирусов всех распространенных типов** - сканирование внутри файлов-документов/таблиц (MS Word, Excel, Office97), упакованных и архивированных файлов. Отсутствие «ложных срабатываний». Возможность лечения зараженных объектов. Для сканеров (см. ниже), как следствие, важной является также периодичность появления новых версий (апдейтов), т.е. скорость настройки сканера на новые вирусы.
- **Существование версий антивируса под все популярные платформы** (DOS, Windows, Windows95, Windows NT, Novell NetWare, OS/2, Alpha, Linux и т.д.), присутствие не только режима «сканирование по запросу», но и «сканирование на лету», существование серверных версий с возможностью администрирования сети.
- **Скорость работы и прочие сервисные опции** (планировщик, фильтры, встроенная помощь, утилиты и т.п.).

Классификация антивирусных программ

- **Программы-детекторы** позволяют обнаружить файлы, зараженные каким-либо известным вирусом
- **Программы-доктора** позволяют не только обнаружить файлы, зараженные известным вирусом, но и произвести их лечение.
- **Программы-ревизоры** запоминают сведения о состоянии программ и системных областей диска компьютера, а затем сравнивают состояние файлов и системных областей диска с исходным.
- **Программы-фильтры**, постоянно находясь в памяти компьютера, следят за действиями, которые выполняются на компьютере. При появлении действий, указывающих на наличие вирусов, они сообщают об этом пользователю.
- **Программы-вакцины** – это программы, предотвращающие заражение файлов. Сущность действия данных программ заключается в том, что они изменяют файлы специальным образом. Причем это не отражается на работе, но вирус воспринимает эти файлы как зараженные и не внедряется в них.