Вредоносное программное обеспечение

Лекция №

Вредоносное ПО

Описание. Классификация.

Вредоносный код -

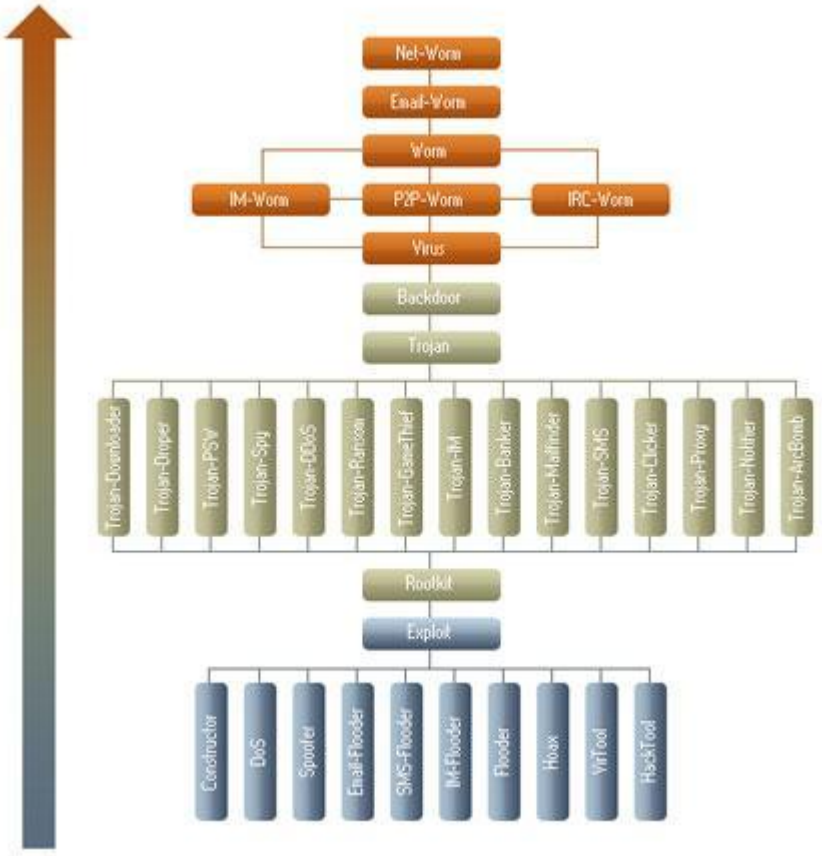
программное обеспечение или его часть, созданное с целью несанкционированного использования ресурсов ПК или причинения вреда владельцу информации, путем копирования, искажения, удаления или подмены информации.

По способу проникновения

- **Собственно вредоносный код** (вирусы)
- Вредоносный код, использующий **уязвимости** ОС или приложений (эксплоиты)
- Вредоносный код, внедряющийся как **часть легального ПО** (программные закладки)

1.Собственно вредоносный код

Классификация вирусов относительно их степени опасности, выполненная в Лаборатории Касперского



2. Уязвимости и эксплоиты

Примеры:

- Переполнения буфера
- Висящие указатели
- SQL-инъекция

Абсолютная защита практически не достижима

3.Программные закладки -

скрыто внедренный код в защищенную систему, который позволяет злоумышленнику осуществлять несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты.

3.Программные закладки

Программные закладки могут:

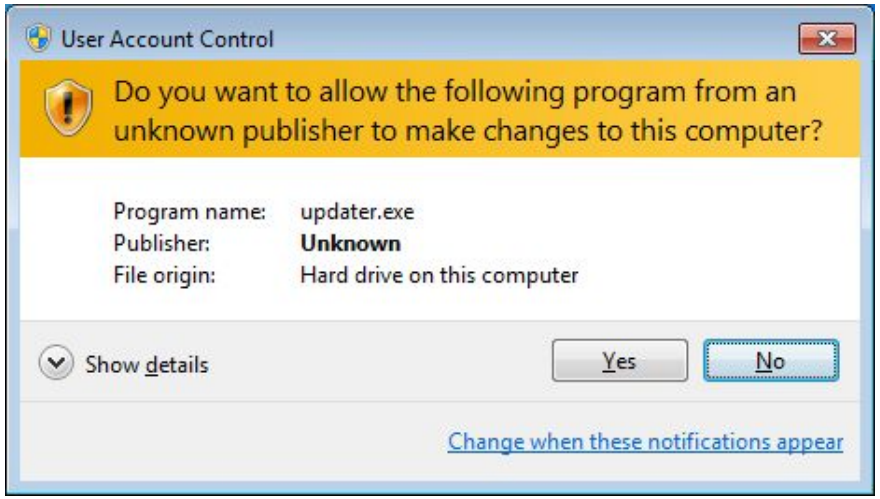
- вносить произвольные искажения в коды программ, находящихся в оперативной памяти компьютера;
- переносить фрагменты информации из одних областей оперативной или внешней памяти компьютера в другие;
- искажать выводимую на внешние компьютерные устройства или в канал связи информацию, полученную в результате работы других программ.

3.Программные закладки

По способу возникновения

Внедренные разработчиком легального ПО

Внедренные из вне (злоумышленником)

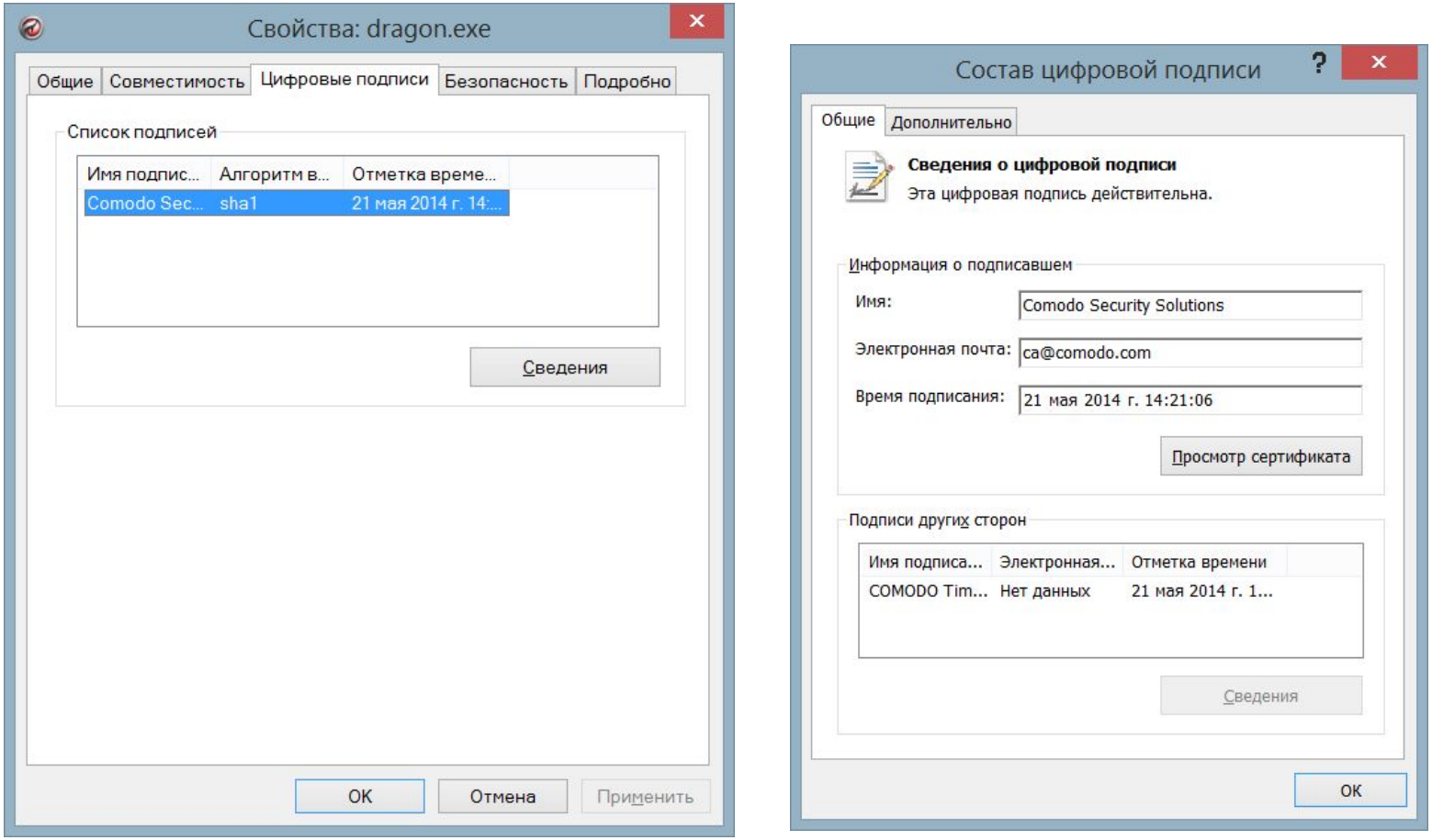


3. Программные закладки

Условия функционирования:

- программная закладка должна попасть в оперативную память;
- должен быть выполнен ряд активизирующих условий, зависящих от типа программной закладки.

3.Программные закладки



Пример подписанного приложения

Вредоносное ПО

Обнаружение. Методы защиты.

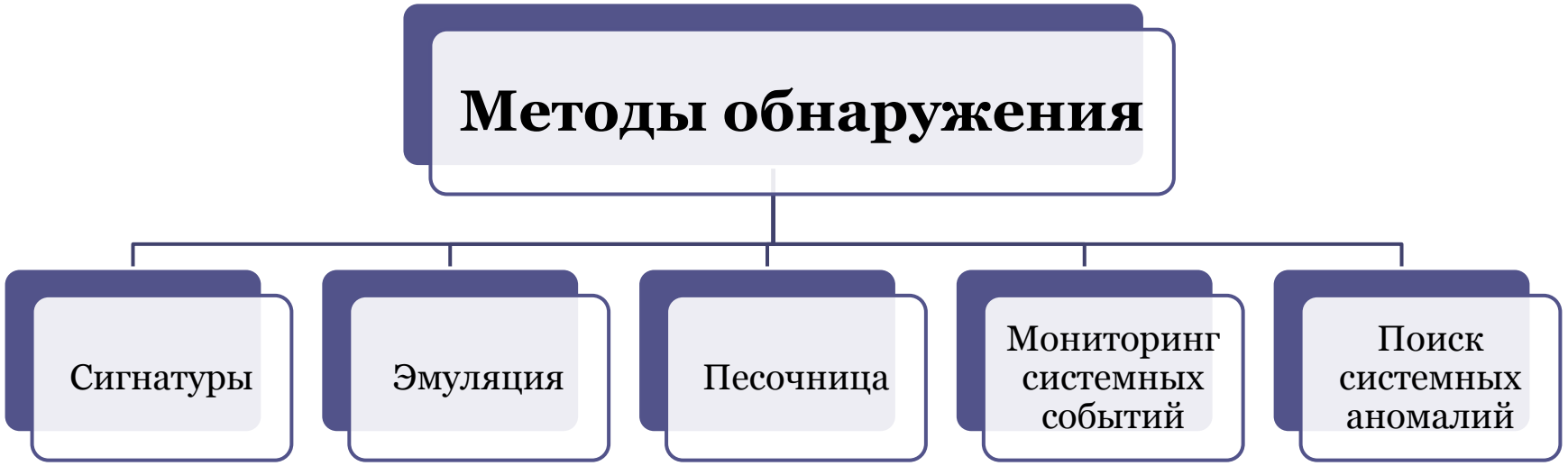
Вредоносный код -

программное обеспечение или его часть, созданное с целью несанкционированного использования ресурсов ПК или причинения вреда владельцу информации, путем копирования, искажения, удаления или подмены информации.

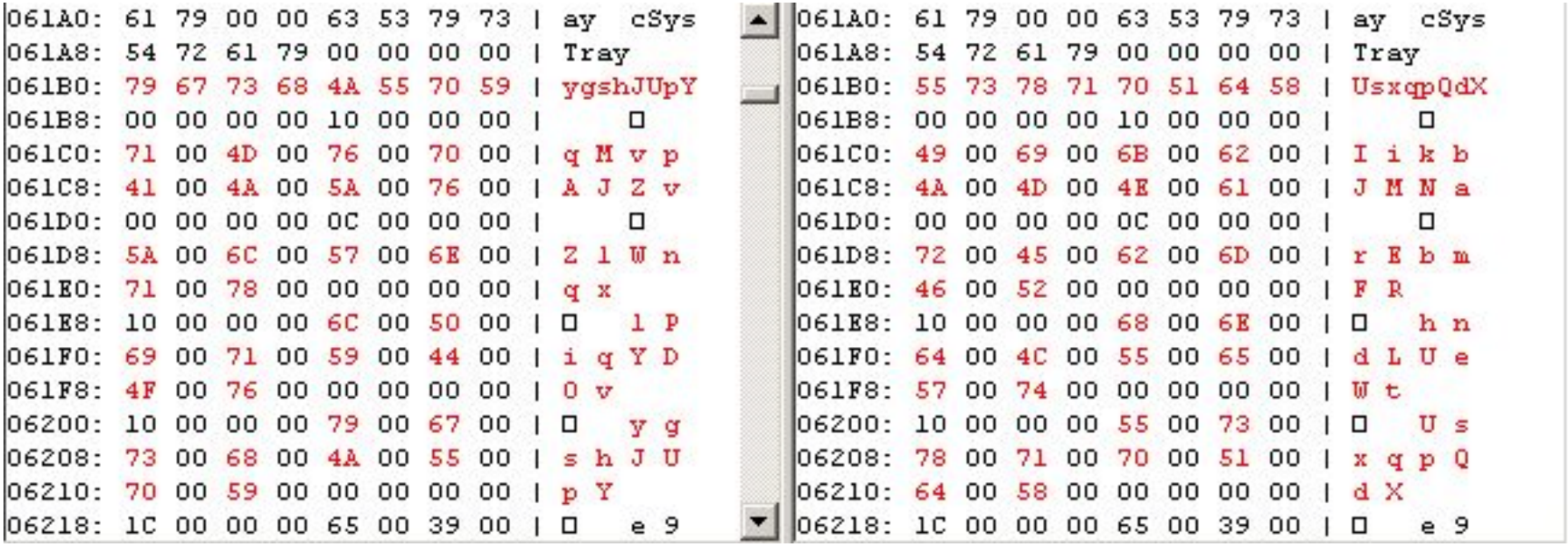
По способу проникновения

- **Собственно вредоносный код** (вирусы)
- Вредоносный код, использующий **уязвимости** ОС или приложений (эксплоиты)
- Вредоносный код, внедряющийся как **часть легального ПО** (программные закладки)

1.Собственно вредоносный код



1. Сигнатуры



```
061A0: 61 79 00 00 63 53 79 73 | ay  cSys
061A8: 54 72 61 79 00 00 00 00 | Tray
061B0: 79 67 73 68 4A 55 70 59 | ygshJUpY
061B8: 00 00 00 00 10 00 00 00 |     □
061C0: 71 00 4D 00 76 00 70 00 | q M v p
061C8: 41 00 4A 00 5A 00 76 00 | A J Z v
061D0: 00 00 00 00 0C 00 00 00 |     □
061D8: 5A 00 6C 00 57 00 6E 00 | Z l W n
061E0: 71 00 78 00 00 00 00 00 | q x
061E8: 10 00 00 00 6C 00 50 00 | □   l P
061F0: 69 00 71 00 59 00 44 00 | i q Y D
061F8: 4F 00 76 00 00 00 00 00 | O v
06200: 10 00 00 00 79 00 67 00 | □   y g
06208: 73 00 68 00 4A 00 55 00 | s h J U
06210: 70 00 59 00 00 00 00 00 | p Y
06218: 1C 00 00 00 65 00 39 00 | □   e 9
```

```
061A0: 61 79 00 00 63 53 79 73 | ay  cSys
061A8: 54 72 61 79 00 00 00 00 | Tray
061B0: 55 73 78 71 70 51 64 58 | UsxqpQdX
061B8: 00 00 00 00 10 00 00 00 |     □
061C0: 49 00 69 00 6B 00 62 00 | I i k b
061C8: 4A 00 4D 00 4E 00 61 00 | J M N a
061D0: 00 00 00 00 0C 00 00 00 |     □
061D8: 72 00 45 00 62 00 6D 00 | r E b m
061E0: 46 00 52 00 00 00 00 00 | F R
061E8: 10 00 00 00 68 00 6E 00 | □   h n
061F0: 64 00 4C 00 55 00 65 00 | d L U e
061F8: 57 00 74 00 00 00 00 00 | W t
06200: 10 00 00 00 55 00 73 00 | □   U s
06208: 78 00 71 00 70 00 51 00 | x q p Q
06210: 64 00 58 00 00 00 00 00 | d X
06218: 1C 00 00 00 65 00 39 00 | □   e 9
```

Сравнение двух копий троянских программ

1. Эмуляция

Эмулятор разбирает байтовый код программы на команды и каждую команду запускает в виртуальной копии компьютера. Это позволяет средству защиты наблюдать за поведением программы, не ставя под угрозу операционную систему и данные пользователя

1. Виртуализация «Песочница»

Виртуализация в том ее виде, в котором она используется в «песочницах», представляет собой логическое продолжение эмуляции. А именно: «песочница» уже работает с исполняющейся в реальной среде программой, но все еще ее контролирует.

1. Мониторинг системных событий

Технически такой способ сбора информации реализуется посредством перехватов функций операционной системы. Таким образом, перехватив вызов некой системной функции, механизм-перехватчик получает информацию о том, что определенная программа совершает определенное действие в системе.

1. Поиск системных аномалий

- Данный метод основан на следующих положениях:
- операционная среда вместе со всеми выполняющимися в ней программами — это интегральная система;
- ей присуще некое «системное состояние»;
- если в среде исполняется вредоносный код, то состояние системы является «нездоровым» и отличается от состояния «здоровой» системы, в которой вредоносного кода нет.

2. Средства анализа уязвимостей

3.Программные закладки

Универсальным средством защиты от внедрения программных закладок является создание *изолированного* компьютера:

- Система использует BIOS, не содержащий программных закладок;
- ОС проверена на наличие закладок;
- Установлена неизменность BIOS и операционной системы для данного сеанса;
- На компьютере не запускалось и не запускается никаких иных программ, кроме уже прошедших проверку на присутствие в них закладок;
- Исключен запуск проверенных программ в каких-либо иных условиях. кроме перечисленных выше, т. е. вне изолированного компьютера.

Общие рекомендации по защите от вредоносного ПО

- Устанавливать минимум ПО
- Загружать ПО из проверенных источников
- Некоторое время мониторить трафик установленного приложения
- Не устанавливать сомнительное ПО