# Классификация вирусов

Alexander Adamov

# Классификация – это важно

- **Классифика́ция** — система — система группировки — система группировки субъектов — система группировки субъектов исследования или наблюдения в соответствии с их общими признаками.
- Классификация объектов производится согласно правилам распределения заданного множества объектов на подмножества (*классификационные группировки*) в соответствии с установленными признаками их различия или сходства

# Определение

- *Определение Евгения Касперского:*

  *ОБЯЗАТЕЛЬНЫМ (НЕОБХОДИМЫМ) СВОЙСТВОМ КОМПЬЮТЕРНОГО ВИРУСА является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера ипрочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.*

- *ГОСТ Р 51188-98:*

  *Вирус – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.*

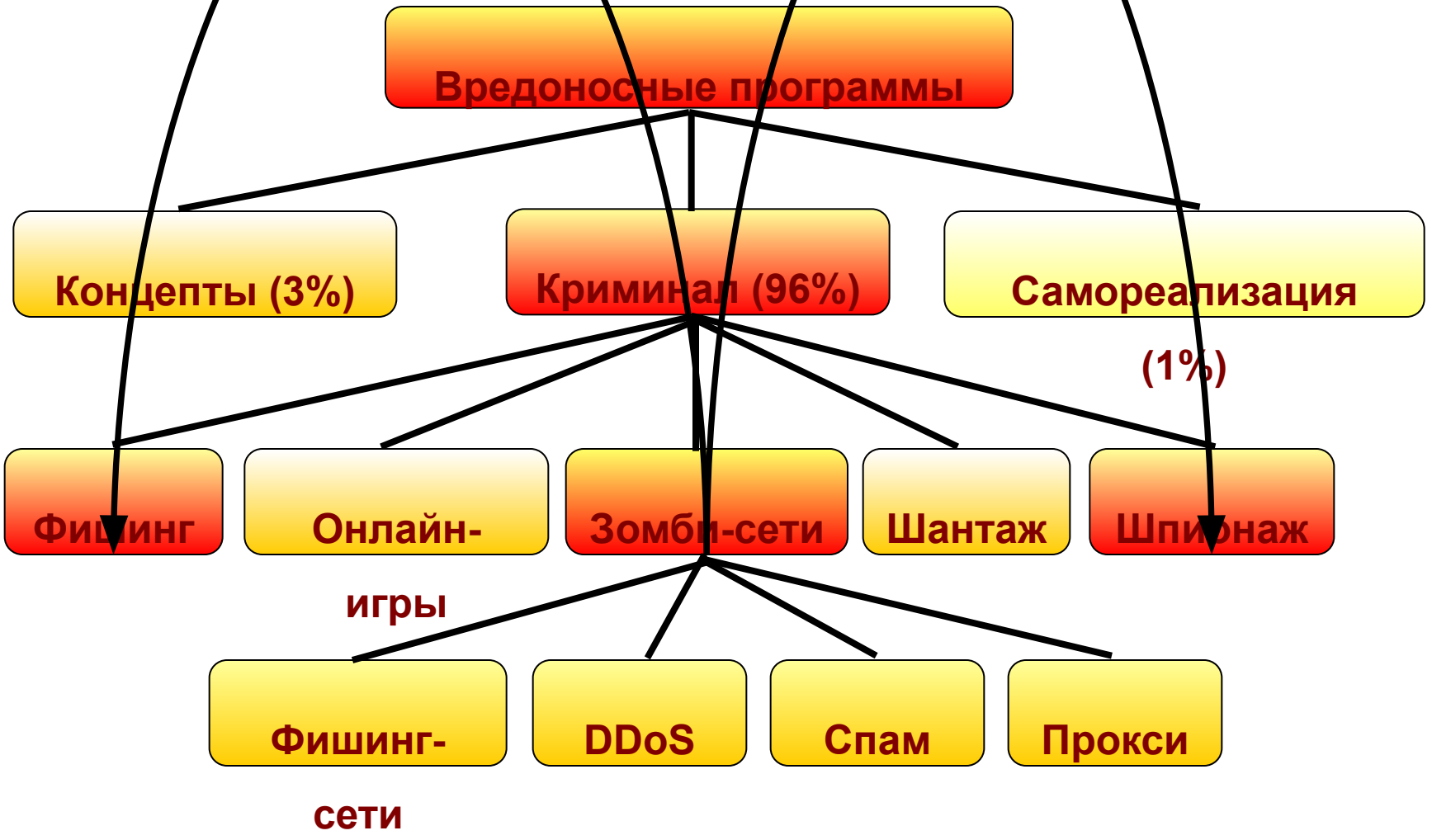
# Определение (2)

- *Вредоносная программа – компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в КС, либо для скрытого нецелевого использования ресурсов КС, либо иного воздействия, препятствующего нормальному функционированию КС.*

# Три группы

- *Вирусы*
- *Трояны*
- *Сетевые черви*

# Классификация угроз



KASPERSKY lab

# ВИРУСЫ

- Жизненный цикл
  1. Проникновение на компьютер
  2. Активация вируса
  3. Поиск объектов для заражения
  4. Подготовка вирусных копий
  5. Внедрение вирусных копий

# Проникновение

- вместе с зараженными файлами или другими объектами, никак, в отличие от червей, не влияя на процесс проникновения.

# Активация

- **Загрузочные вирусы** – вирусы, заражающие загрузочные сектора постоянных и сменных носителей (Virus.Boot.Snow.a, Virus.Boot.DiskFiller)
- **Файловые вирусы** – вирусы, заражающие файлы.
  а) Собственно файловые вирусы (Virus.Win9x.CIH)
  б) Макровирусы (Macro.Word97.Thus)
  в) Скриптвирусы (Virus.VBS.Sling)

# Поиск жертв

1. Получив управление, вирус производит разовый поиск жертв, после чего передает управление ассоциированному с ним зараженному объекту (Virus.Multi.Pelf.2132)
2. Получив управление, вирус так или иначе остается в памяти и производит поиск жертв непрерывно, до завершения работы среды, в которой он выполняется (Virus.DOS.Anarchy.6093)

# Подготовка копий

KASPERSKY lab

## Технологии маскировки:

- **Шифрование**
- **Метаморфизм**

## Результат:

- **Шифрованный вирус**
- **Метаморфный вирус**
- **Полиморфный вирус (**Virus.Win32.Etap**)**

# Внедрение

2 метода:

- Внедрение вирусного кода непосредственно в заражаемый объект
- Замена объекта на вирусную копию. Замещаемый объект, как правило, переименовывается (вирус-компаньон Email-Worm.Win32.Stator.a)

# ЧЕРВИ

# Черви

- Определение:

  *Червь (сетевой червь) – тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, и осуществлению иного вредоносного воздействия.*

# Жизненный цикл

- Жизненный цикл
  - Проникновение в систему
  - Активация
  - Поиск «жертв»
  - Подготовка копий
  - Распространение копий

# Каналы распространения

**По типу используемых протоколов:**

- **Сетевые черви**
- **Почтовые черви**
- **IRC-черви**
- **P2P-черви**
- **IM-черви**

# Активация

1. Для активации необходимо активное участие пользователя
2. Для активации участие пользователя не требуется вовсе либо достаточно лишь пассивного участия

# Поиск жертв

На основе используемых протоколов:

1. Сканирование IP-адресов
2. Адресная книга почтовых клиентов
3. Список контактов интернет-пейджеров и IRC-клиентов
4. Каталоги общего доступа пиринговых сетей

# Подготовка копий

Такие же как и у вирусов.

Наиболее популярный метод:

- Упрощенный метаморфизм (черви могут менять тему и текст инфицированного сообщения, имя, расширение и даже формат вложенного файла)

# ТРОЯНЫ

# Трояны

- Определение:

  *Троян (троянский конь) – тип вредоносных программ, основной целью которых является вредоносное воздействие по отношению к компьютерной системе. Трояны отличаются отсутствием механизма создания собственных копий. Некоторые трояны способны к автономному преодолению систем защиты КС, с целью проникновения и заражения системы. В общем случае, троян попадает в систему вместе с вирусом либо червем, в результате неосмотрительных действий пользователя или же активных действий злоумышленника.*

# Жизненный цикл

Жизненный цикл

- Проникновение на компьютер
- Активация
- Выполнение заложенных функций

# Способы проникновения

1. **Маскировка**
   (Trojan.SymbOS.Hobble.a)

2. **Кооперация с вирусами и червями**

# Активация

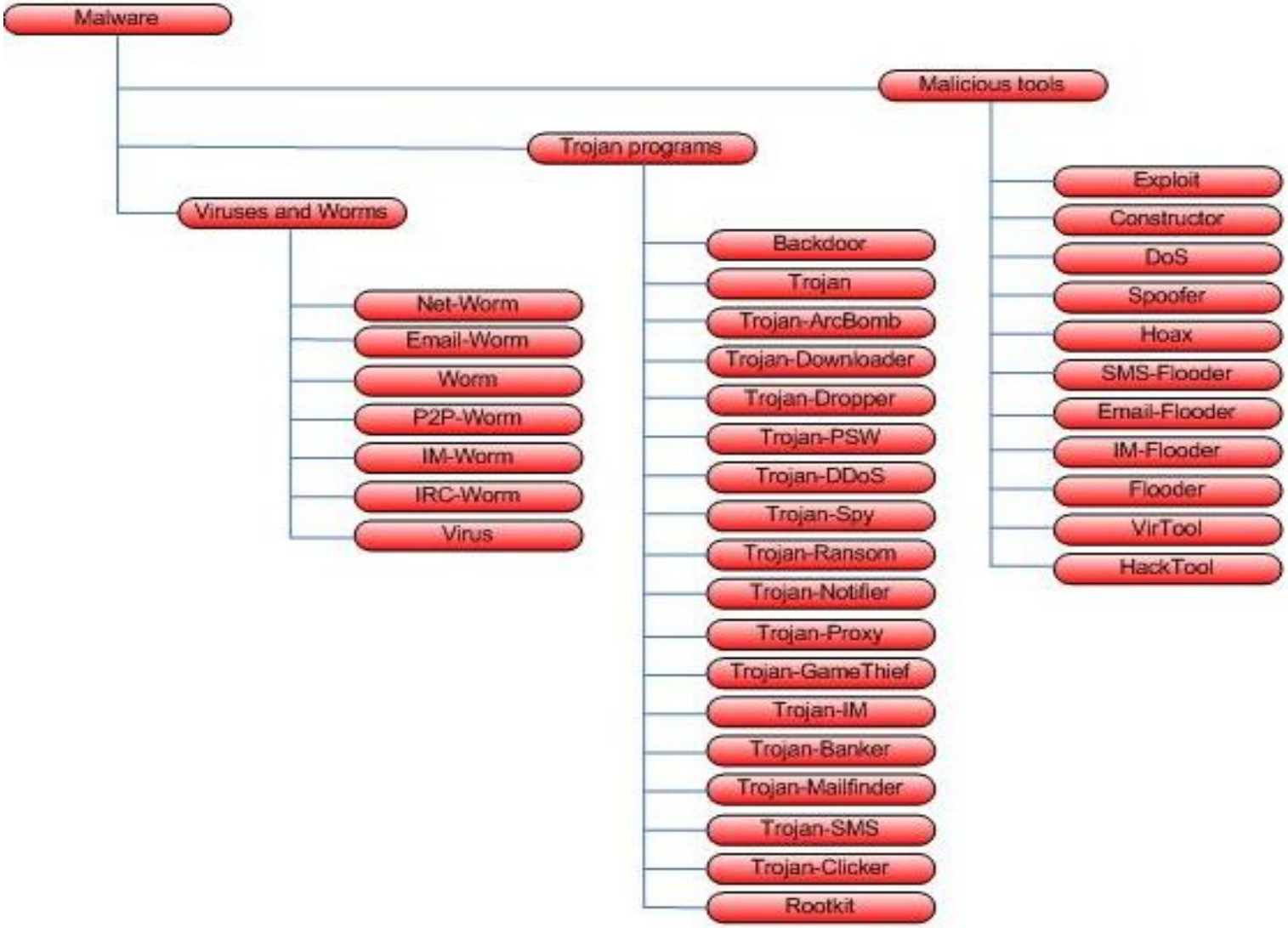
Тоже что и у червей:

- Для активации необходимо активное участие пользователя
- Для активации участие пользователя не требуется вовсе либо достаточно лишь пассивного участия

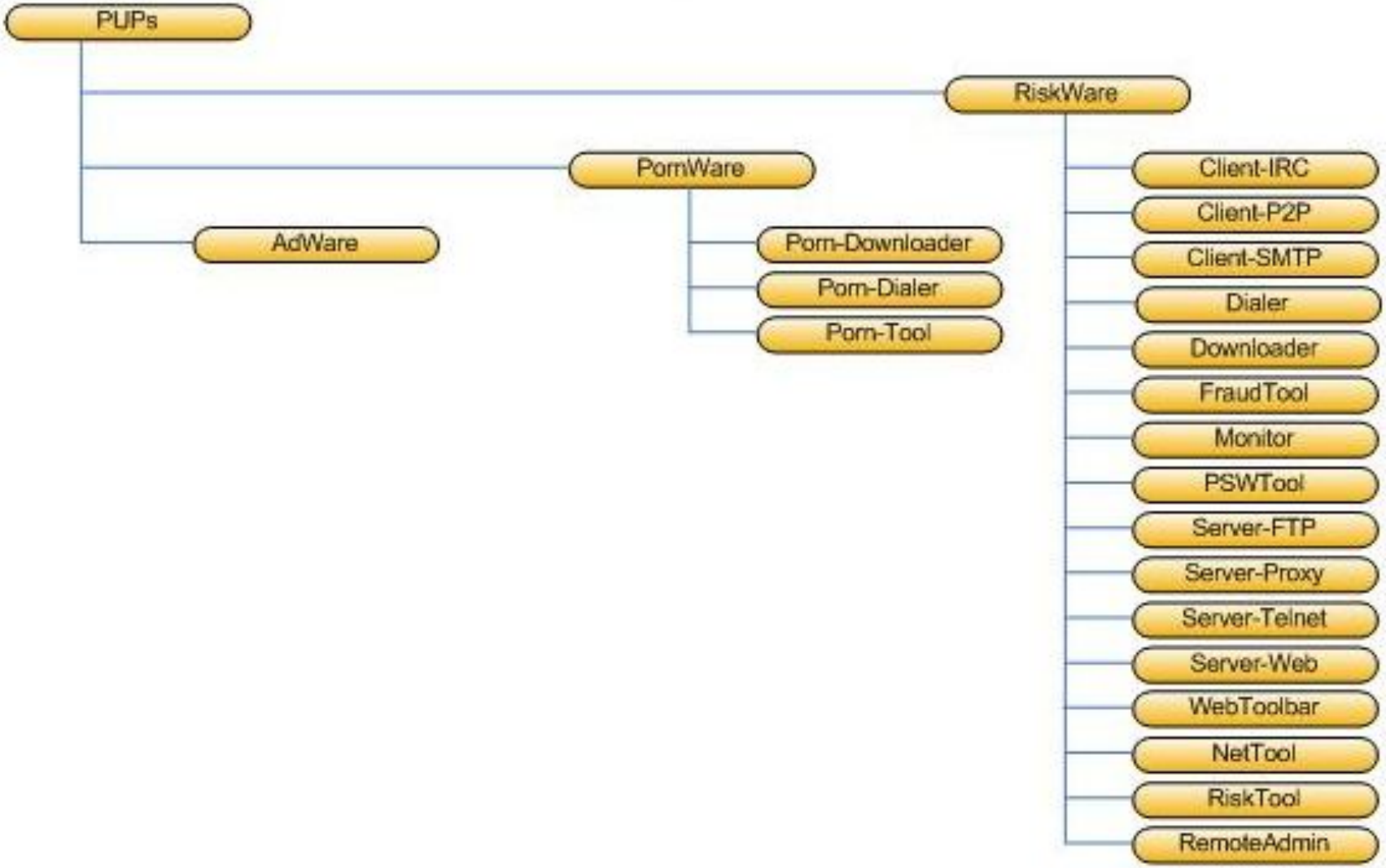
# Функционал

- Клавиатурные шпионы (Keylogger)
- Похитители паролей (Trojan-PSW)
- Утилиты удаленного управления (Backdoor)
- Анонимные smtp-сервера и прокси (Trojan-Proxy)
- Утилиты дозвона (Trojan-Dialer)
- Модификаторы настроек браузера (Trojan-Clicker, Trojan-StartPage)
- Логические бомбы (Virus.Win9x.CIH, Macro.Word97.Thus)

# Новая классификация



# Новая классификация (2)



# Правила именования

## Behaviour.OS.Name[.Variant..]

- **Behaviour** - определяет поведение детектируемого объекта. Для вирусов и червей поведение определяется по способу распространения, для троянских программ и malicious tools поведение определяется по совершаемым ими несанкционированным пользователем действиям. Для PUP- по функциональному назначению детектируемого объекта.
- **OS** - операционная система, под которой выполняется вредоносный или потенциально-нежелательный программный код.
- **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’, ...

  *Variant не является обязательным в имени и может отсутствовать

# Вопросы?

Alexander Adamov

KASPERSKY lab