ВРЕДОНОСНОЕ ПО И МЕТОДЫ БОРЬБЫ С НИМ

Глава 1
Что такое вредоносное программное обеспечение

Вредоносное ПО (MalWare)

Malware

Вредоносные программы, созданные специально для несанкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей. К данной категории относятся вирусы, черви, троянские программы и иной инструментарий, созданный для автоматизации деятельности злоумышленников (инструменты для взлома, конструкторы полиморфного вредоносного кода и т.д.).

Классификация вредоносного ПО

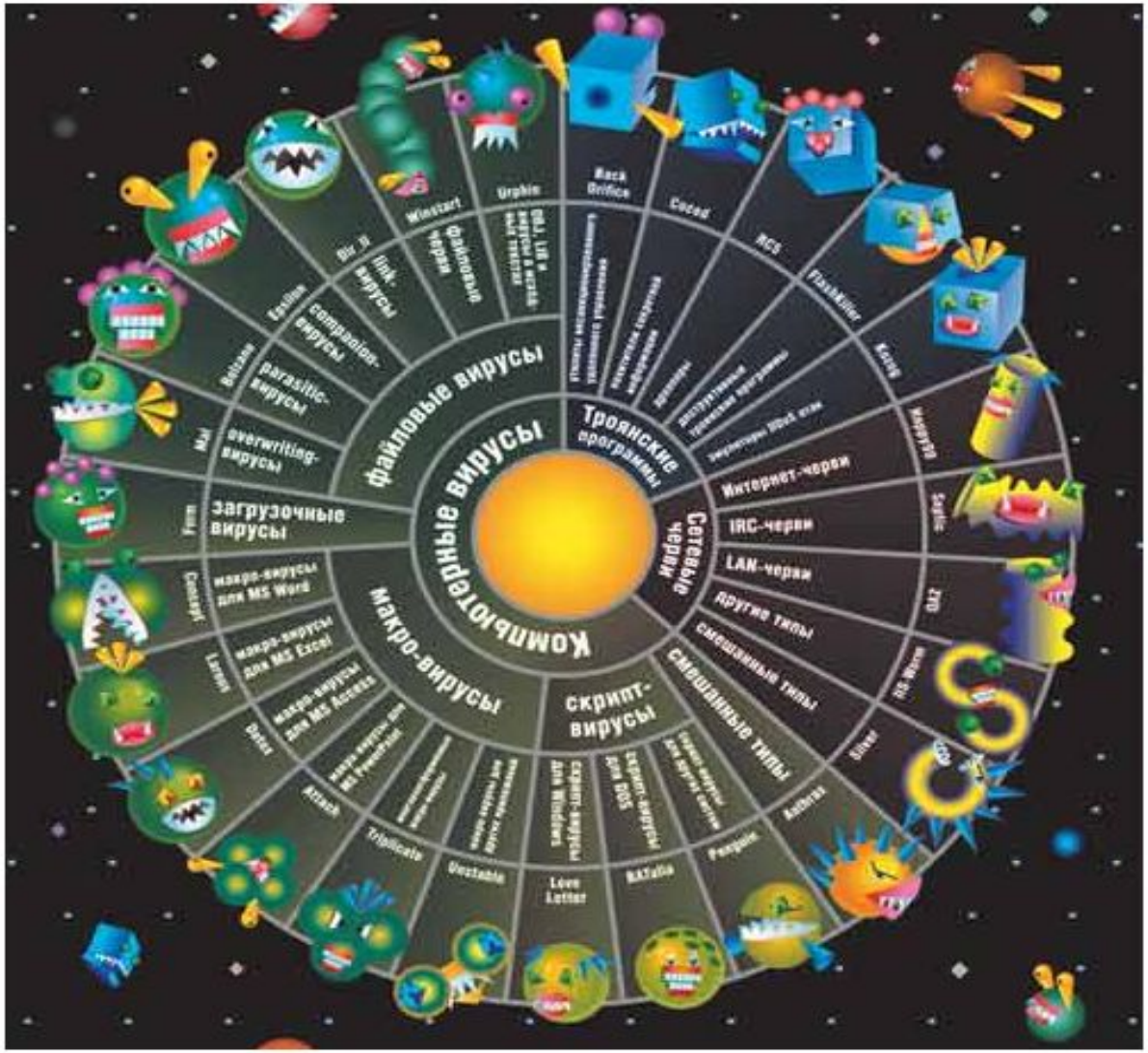


Рис. 1. Классификация вредоносных программ (источник: «Лаборатория Касперского»)

Российское законодательство (УК РФ)

- Статья 272. Неправомерный доступ к компьютерной информации.
- Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.
- Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Компьютерные угрозы

- Вредоносные программы
- Спам
- Сетевые атаки (хакеры)
- Внутренние угрозы (инсайдеры)

  - утечка/потеря информации (в т.ч. финансовой)
  - нештатное поведение ПО
  - резкий рост входящего/исходящего трафика
  - замедление или полный отказ работы сети
  - потеря времени
  - доступ злоумышленника в корпоративную сеть
  - риск стать жертвой мошенников

Криминализация индустрии

- Похищение конфиденциальной информации
- Зомби-сети (ботнеты)
  - рассылка спама
  - DDoS-атаки
  - троянские прокси-серверы
- Шифрование пользовательской информации с требованием выкупа
- Атаки на антивирусные продукты
- Флашинг (PDoS – Permanent Denial of Service)

Похищение конфиденциальной информации

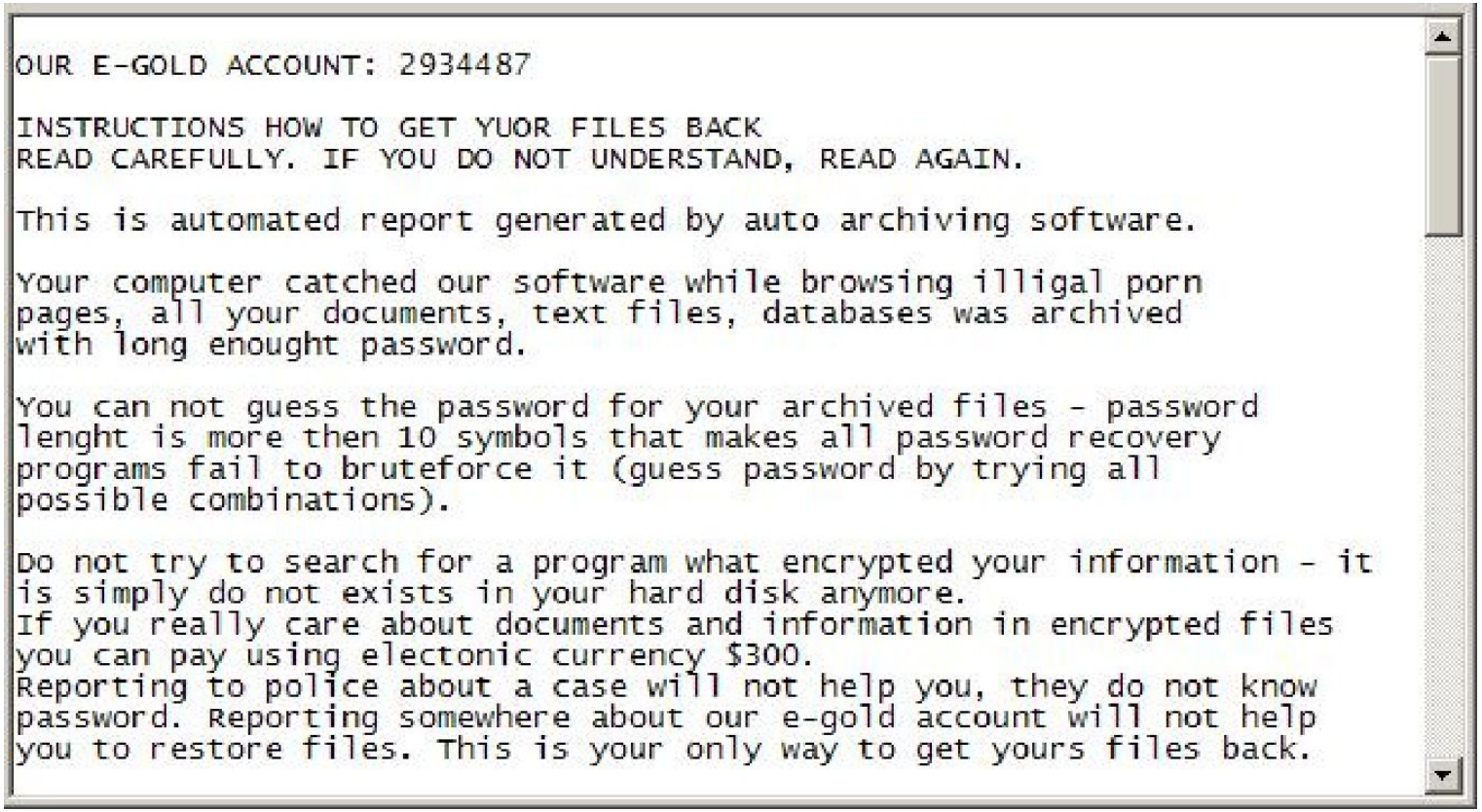
- Документы и данные
- Учетные записи и пароли
  - он-лайн банки, электронные платежи, интернет-аукционы
  - интернет-пейджеры
  - электронная почта
  - интернет сайты и форумы
  - он-лайн игры
- Адреса электронной почты, IP-адреса

Зомби-сети (ботнеты)

- Программа-загрузчик
  - распространение собственного кода и кода программы бота
- Программа-бот
  - сбор и передача конфиденциальной информации, рассылка спама, участие в DDoS-атаке и т.д.
- Управляющий ботнет
  - сбор информации от ботов и рассылка «обновлений» для них

Шифрование пользовательской информации с требованием выкупа за расшифровку

- Требование выкупа от троянской программы “Cryzip”



```
OUR E-GOLD ACCOUNT: 2934487

INSTRUCTIONS HOW TO GET YUOR FILES BACK
READ CAREFULLY. IF YOU DO NOT UNDERSTAND, READ AGAIN.

This is automated report generated by auto archiving software.

Your computer catched our software while browsing illigal porn
pages, all your documents, text files, databases was archived
with long enought password.

You can not guess the password for your archived files - password
lenght is more then 10 symbols that makes all password recovery
programs fail to bruteforce it (guess password by trying all
possible combinations).

Do not try to search for a program what encrypted your information - it
is simply do not exists in your hard disk anymore.
If you really care about documents and information in encrypted files
you can pay using electonic currency $300.
Reporting to police about a case will not help you, they do not know
password. Reporting somewhere about our e-gold account will not help
you to restore files. This is your only way to get yours files back.
```

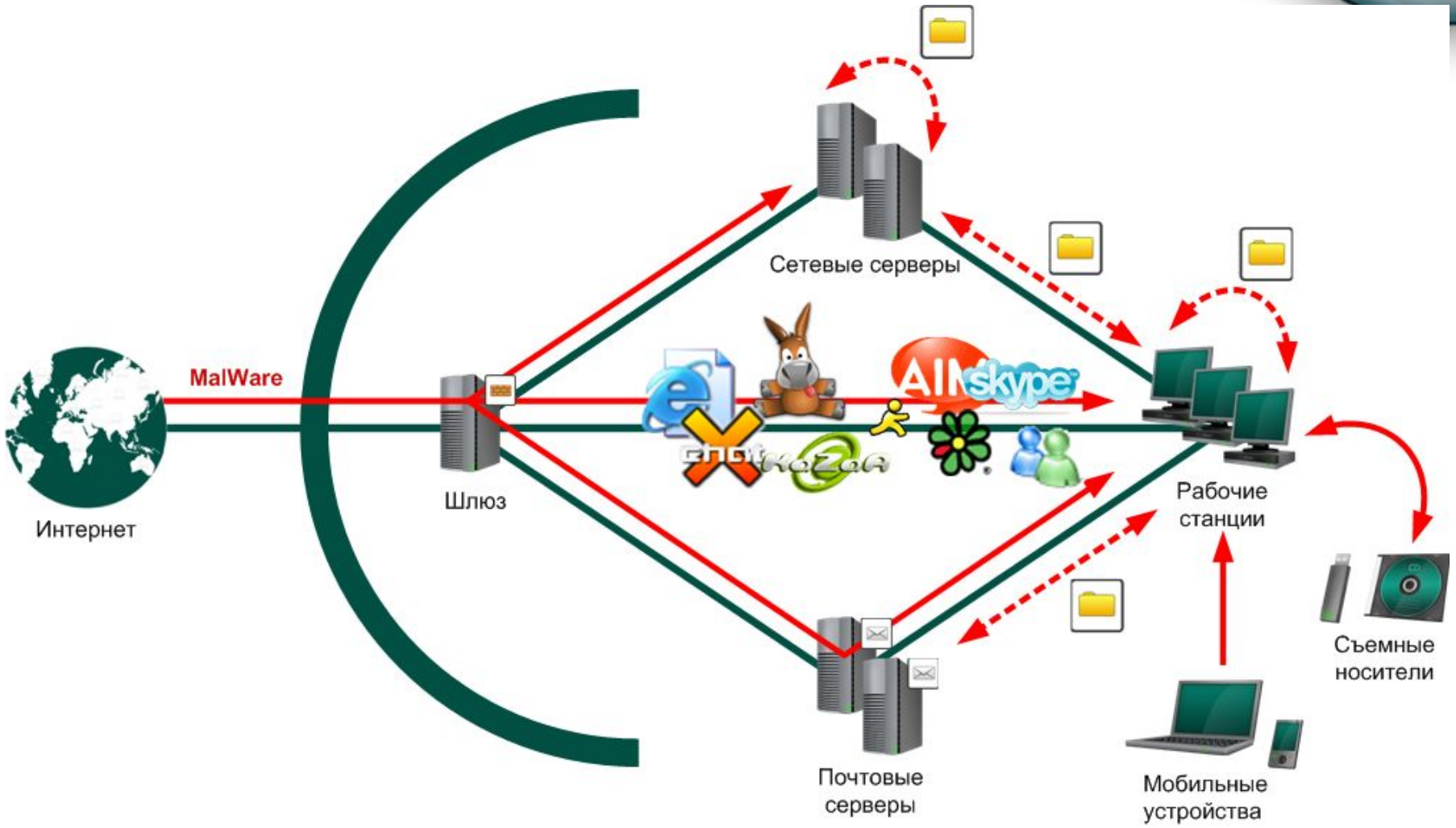
Противодействие антивирусным технологиям

- Остановка работы антивируса
- Изменение настроек системы защиты
- Авто-нажатие на клавишу “Пропустить”
- Сокрытие присутствия в системе (руткиты)
- Затруднение анализа
  - шифрование
  - обфускация
  - полиморфизм
  - упаковка

Каналы распространения вредоносного ПО

- Электронная почта
- Интернет-сайты
- Интернет-пейджеры
- Социальные сети
- Сети передачи данных
- Физический перенос данных

Типичная схема заражения



Глава 2
Основные виды вредоносных программ

VirWare
(классические вирусы и сетевые черви)

Классические компьютерные вирусы

- Запуск при определенных событиях
- Внедрение в ресурсы системы
- Выполнение необходимых действий

Классификация вирусов

- По среде обитания
  - Файловые вирусы
  - Загрузочные вирусы
  - Макро-вирусы
  - Скриптовые вирусы

Файловые вирусы

Способы заражения

- Перезаписывающие (overwriting)
- Паразитические (parasitic)
- Заражающие объектные модули (OBJ)
- Вирусы-компаньоны (companion)
- Заражающие библиотеки компиляторов (LIB)
- Вирусы-ссылки (link)
- Заражающие исходные тексты программ

Загрузочные вирусы

- Модифицируют загрузочный сектор диска
- Перехватывают управление при запуске ОС

- В настоящий момент слабо распространены

Макро-вирусы

- Используют возможности макро-языков
- Заражают область макросов электронных документов

- Наиболее распространены в среде Microsoft Office

Расположение макро-вируса в документе

Незараженный файл (документ или таблица)	Зараженный файл (документ или таблица)
Заголовок файла	Заголовок файла
Служебные данные (каталоги, FAT)	Служебные данные (каталоги, FAT)
Текст	Текст
Шрифты	Шрифты
Макросы (если есть)	Макросы (если есть) ---------- Макросы вируса
Прочие данные	Прочие данные

Скрипт-вирусы

- Пишутся на скрипт-языках
  - VBS, JS, PHP, BAT и т.д.
- Заражают скрипт-программы (командные и служебные файлы ОС)
- Могут входить в состав многокомпонентных вирусов

- Наиболее распространены в интернет

Сетевые черви

- Проникновение на удаленные компьютеры
- Выполнение необходимых действий
- Распространение своих копий

Классификация сетевых червей

Email-Worm
(почтовые черви)

IRC-Worm
(черви в IRC-каналах)

IM-Worm
(черви, использующие интернет-пейджеры)

P2P-Worm
(черви для сетей обмена файлами)

Net-Worm
(прочие сетевые черви)

TrojWare
(троянские программы)

Троянские программы

- Скрытый сбор/модификация информации
- Передача данных злоумышленнику
- Использование ресурсов компьютера без ведома пользователя

Классификация троянских программ

Backdoor	(удаленное администрирование)	30%
Trojan-Downloader	(доставка вредоносных программ)	20%
Trojan	(прочие троянские программы)	18%
Trojan-PSW	(воровство паролей)	17%
Trojan-Spy	(шпионские программы)	7%
Trojan-Dropper	(инсталляторы вредоносных программ)	6%
Trojan-Clicker	(интернет-кликеры)	1%
Trojan- Proxy	(троянские прокси-серверы)	<1%
Rootkit	(сокрытие присутствия в ОС)	<1%
Trojan-DDoS	(распределенные атаки)	<1%
Trojan-SMS	(«мобильные троянцы»)	<1%

Руткиты (Rootkit) в Windows

- Модификация обработчиков системных функций (Windows API)

- Сокрытие процессов в диспетчере задач

Suspicious packers (подозрительные упаковщики)

- Вредоносные программы сжимаются различными способами упаковки, совмещёнными с шифрованием содержимого файла для того, чтобы исключить обратную разработку программы и усложнить анализ поведения проактивными и эвристическими методами.

Основные признаки:

-вид упаковщиков

-количество упаковщиков

Классификация подозрительных упаковщиков

MultiPacked (многократно упакованные)

SuspiciousPacker (сжатые упаковщиками, созданными специально для защиты вредоносного кода от детектирования антивирусными ПО)

RarePacker (сжатые редко встречающимися упаковщиками)

Malicious tools
(программы для создания вредоносного ПО)

- Вредоносные программы, разработанные для автоматизированного создания вирусов, червей и троянских программ, организации DoS-атак на удалённые сервера, взлома других компьютеров и т.п.

Основной признак:

-совершаемые ими действия

Классификация Malicious tools

Constructor (изготовление нового вредоносного ПО)

DoS (проведение DoS-атак)

Email-Flooder (переполняют бесполезными сообщениями каналы электронной почты)

IM-Folder (переполняют бесполезными сообщениями каналы интернет-пейджеров)

SMS-Flooder (переполняют бесполезными сообщениями каналы SMS-сообщений)

Flooder (переполняют бесполезными сообщениями сетевые каналы)

Spoofer (подменяют адрес отправителя в сообщениях)

VirTool (модифицируют другие вредоносные программы таким образом, чтобы они не детектировались антивирусным ПО)

Hoax («злые шутки»)

HackTool (используется при организации атак на компьютер)

Potentially Unwanted Programs, PUPs (условно опасные программы)

Условно опасные программы (PUPs)

- Разрабатываются и распространяются легальными компаниями
- Могут использоваться в повседневной работе
  - утилиты удаленного администрирования и т.п.
- Обладают набором потенциально опасных функций
- Могут быть использованы злоумышленником

PUPs

RiskWare
(легальные потенциально опасные программы)

AdWare
(рекламное ПО)

PornWare
(показ информации порнографического характера)

RiskWare

- Утилиты удаленного администрирования
- Программы-клиенты IRC
- Звонилки-дайлеры
- Скачиватели-даунлоадеры
- Мониторы любой активности
- Утилиты для работы с паролями
- Интернет-серверы служб FTP, Web, Proxy, Telnet

AdWare

- Показывают нежелательные рекламные сообщения
- Перенаправляют поисковые запросы на рекламные веб-страницы
- Скрывают свое присутствие в системе
- Встраивают рекламные компоненты в бесплатное и условно-бесплатное ПО

AdWare: утечка информации

- IP-адрес компьютера
- Версия ОС и интернет-браузера
- Список часто посещаемых ресурсов
- Поисковые запросы
- Прочие данные, которые можно использовать в рекламных целях

Распределение новых вредоносов по платформам (2008)

Windows	439922	99,912%
*nix	230	0,052
Mac	20	0,005
Mobile	88	0,020
Прочие	51	0,012

- *nix: FreeBSD, Linux, Perl, PHP, Ruby, Unix
- Mobile: Python, Symbyan
- Прочие: BeOS, Boot, Boot-DOS, MS-DOS, Multi, SAP, SQL, SunOS

Признаки заражения (MalWare)

- Наличие autorun.inf файлов в корнях дисков
- Блокирование доступа к антивирусным сайтам
- Изменение файла hosts
- Блокирование запуска антивирусных программ
- Несанкционированное открытие веб-страниц
- Измененная стартовая страница браузера
- Всплывающие окна в браузере
- Отключение стандартных служб Windows
- Интенсивная дисковая или сетевая активность
- Установленные программы не запускаются


Спасибо за внимание!