

Компьютерные угрозы – классификация, история возникновения

Сергей Новиков

Руководитель российского центра исследований

- История возникновения вредоносных программ
- Современные интернет-угрозы
- Путь зловреда к аналитикам
- Классификация ЛК
- Будущее

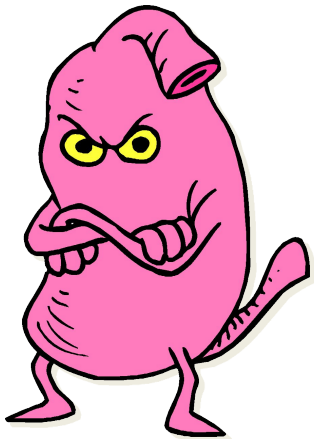


Дела давно минувших дней

Ранняя история вирусов

- **Вирус – компьютерная программа, которая может распространяться (копировать себя)**
- **Дополнительно, вирус может заражать системные ресурсы (CodeRed.A), портить данные (I-Worm.Klez), компроментировать секретную информацию (I-Worm.Sircam) и стирать flash-BIOS (Win95.CIH).**

Я, компьютерная программа,
специально разработанная
для проведения
неавторизованных действий,
таких как аномальное
поведение компьютера,
модификация, уничтожение
или кража данных





1836

Charles Babbage



Теория саморазмножающихся механизмов

1951

John von Neumann

Двумя моделями само множащихся механизмов ("Scientific American")

1959

L.S. Penrose



Практическая реализация модели на IBM 650

F.G. Stahl

ку, G.MacIlroy, R.Morris Создают игру «Дарвин»

1962

Bell Labs

Дальше - больше

Creeper/
Reaper
в ARPAnet

"R
майнфреймах

На Apple 2

"Виррус"

"Brain":
Первый
бут вирус
для IBM PC

1970

1974

1975

1981

1983

1986

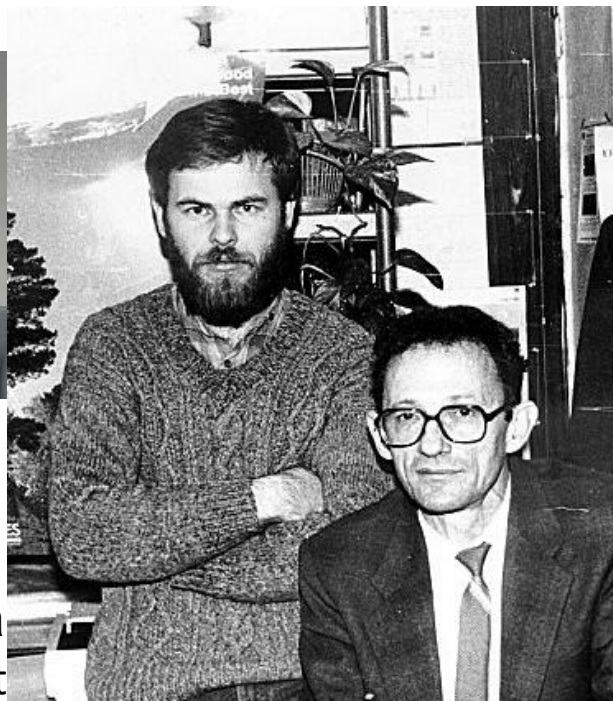
Fred Kohen

Basit Farooq Alvi



- Первый PC вирус – буттовый вирус
- Boot.Brain заражал загрузочные сектора дискет и MBR на HDD
- Буттовые вирусы были очень «популярны» до наступления эры Internet, когда флоппи диски были единственным средством обмена файлами
- Сейчас, загрузочные вирусы больше не проблема, однако появились «внуки» – буткиты.

Средние века



“Virdem”:
COM - вирус

Эпидемия
вируса
«Jerusalem»
RCE-1813

Червь
Морриса
ARPAnet

“Win.Vir_1_4”
– первый
вирус для
Windows

1986

1987

1988

1989

1990

1992

Ralf Burger

- После загрузочных вирусов появились вирусы, заражающие исполняемые файлы (для MS-DOS это были .COM, .EXE и .SYS файлы)
- Файлово-загрузочные вирусы тоже появились – Tequila.2468, OneHalf.3544
- Такие вирусы наиболее быстро распространялись и наносили наибольший вред

Malware. История: «Новая история»



- Макро вирусы – первый был обнаружен в 1995 (WM/Concept.A, хотя говорят, что был написан в 1994)
- Был разрушен миф о том, что документы не могут быть заражены вирусами
- Быстро стали «головной болью» для всех.
- Макро вирусы написаны для всех популярных VBA приложений
- 26 марта 1999 – впервые применена новая технология распространения, которая с успехом используется и в наши дни

- Macro.Word97.Melissa был первым вирусом, который распространился по всему миру за один день
- Технология была перенесена на скрипт язык VBS, сделав скрипт вирусы №1 по популярности на многие годы
- Наиболее известными скрипт вирусами были VBS.LoveLetter, VBS.VBSWG (Курникова)

Увеличение количества Win32 вирусов

- Улучшившая защищенность приложений MS Office и VBS, свела на нет «популярность» таких вирусов в 2001-2002 годах
- Win32 mass mailers стали очень «популярны» в 2000 (Win32.Ska, Win32.MyPics или Win32.ExploreZip)

- Один из самых первых «современных» интернет червей – червь Морриса, заражавший Sun и VAX компьютеры. 1988 год
- Идея распространения программ по сети (не почта!) была переоткрыта в 2000 – червь VBS.Netlog
- Черви для локальных сетей (в дополнение к Internet-червям) также были разработаны (Win32.ExploreZip)

История: «Новейшая история»

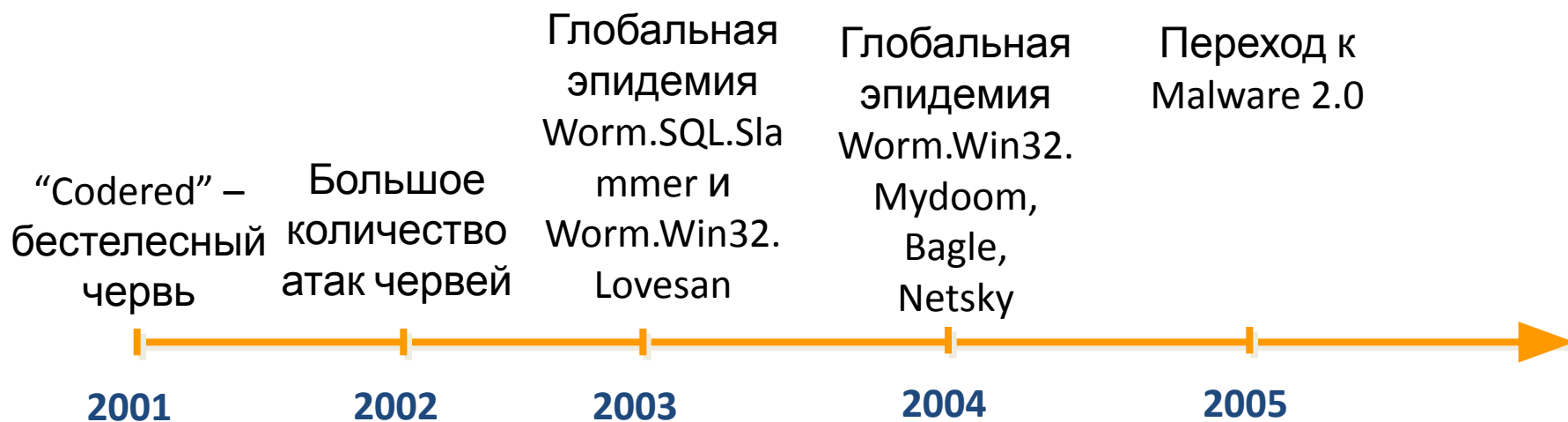


“Cod
бесте
че
20



* 14 августа
2003

Malware. История: «Новейшая история»

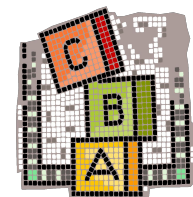


Настоящее время

Malware 2.0

Malicious software

- Вирусы
Заражают файлы
- Черви
Распространяются с компьютера на компьютер
- Троянцы
Не могут сами распространяться
- Вредоносные утилиты
Используются авторами вирусов
e.g. Упаковщики, конструкторы, эксплоиты



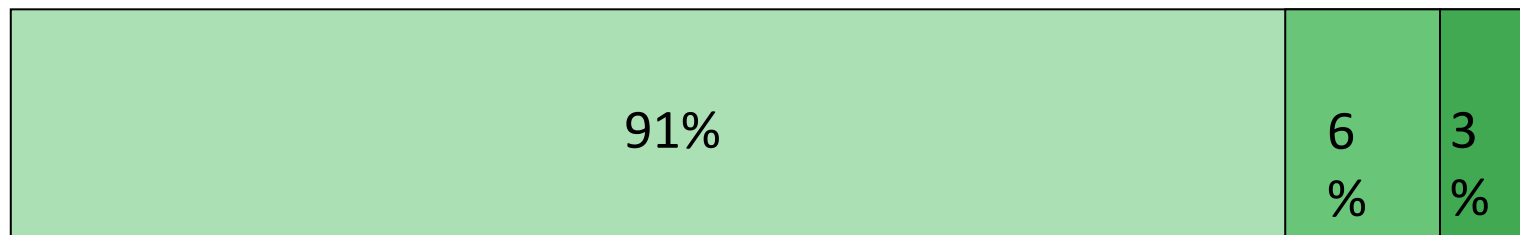
- 2004 - Bagle
- 2006 – Warezov
- 2007 – Zhelatin aka Storm Worm
- 2008 – Буткит Sinowal
- 2009 - Kido aka Conficker

- Отказ от массовых рассылок
- Отказ от распространения через порты
- Использование скрипт-языков
- Новое использование старых технологий
- Zero-minute
- DDoS
- Phishing

- РНР внедрения
- SQL injections
- DNS poisoning/pharming
- Атаки на социальные сети

- Фишинг изменился в сторону нацеленности на пользователей социальных сетей.
- Учетные данные абонентов Facebook, Вконтакте, Livejournal, Одноклассники и др., пользуются повышенным спросом у злоумышленников.
- XSS\PHP\SQL-атаки.
- Цель – приватные данные и создание баз \ списков для проведения последующих атак при помощи «традиционных» способов.

Статистика



Trojans



Viruses & worms



Malicious tools

Путь зловреда к аналитикам

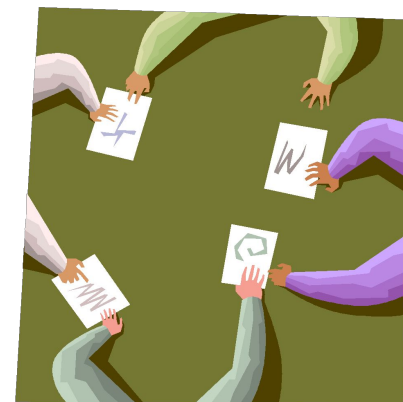
Newvirus, collection exchange, облака

- Newvirus@kaspersky.com
- 24 часа/7 дней в неделю/365 дней в году
- Тысячи писем в сутки с In-the-Wild зловредами от людей со всего мира



Главная задача – защитить пользователя!

- Collection exchange
 - Участники:
AVG, ClamAV, Comodo, ESET, F-secure, Frisk, Kaspersky, Kingsoft, McAfee, Sophos, Symantec, TrendMicro...
 - **~10 Терабайт** вредоносных файлов в квартал



- KSN [Kaspersky Security Network] - новая технология защиты
- >60 Миллионов участников
- Real-time система расчета репутации файлов
- Известны **ИСТОЧНИКИ** вредоносных и подозрительных файлов



История классификации

В поисках подходов к классификации

- Схема именования Н.Н. Безрукова (1990 год)
- Схема именования «CARO» V. Bontchev (1991/2002 год)
- CME (Common malware Enumeration) –уникальный ID для одинаково детектируемых объектов
- Классификации антивирусных компаний

- Различные классификации AV-компаний
- Различные классификации тестеров
- Много тяжело-воспринимаемых или неинформативных классификаций
- Найти пересечения названий очень тяжело

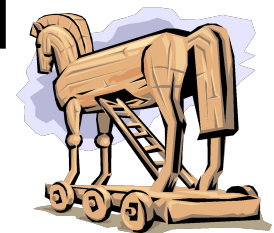
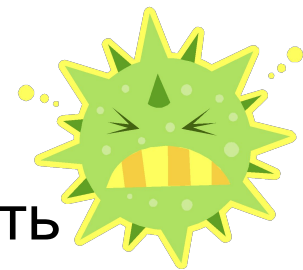
Подход Лаборатории Касперского

Дерево, именование, альтернативы

Нужно детектировать только вредоносные программы?

Malware (Malicious software)

- Вирусы и Черви [Способ распространения]
 - Вирусы по локальным ресурсам не используя сеть
 - Черви размножаются используя сеть
- Троянские программы [Совершаемые действия]
 - различные вредоносные действия, но никакого самораспространения
- Вредоносные утилиты [Совершаемые действия]
 - Используются авторами вредоносов
 - Например: пакеры, конструкторы, флудеры и т.п.



Malware



Malware

Viruses and Worms

- Email-Worm
- IM-Worm
- IRC-Worm
- Net-Worm
- P2P-Worm
- Virus
- Worm

Trojan programs

- Backdoor
- Rootkit
- Trojan-ArcBomb
- Trojan-Banker
- Trojan-Clicker
- Trojan-DDoS
- Trojan-Downloader
- Trojan-Dropper
- Trojan-GameThief
- Trojan-Ransom
- Trojan-IM
- Trojan-Mailfinder
- Trojan-Notifier
- Trojan-Proxy
- Trojan-PSW
- Trojan-SMS
- Trojan-Spy
- Trojan

Malicious tools

- Constructor
- DoS
- Exploit
- Email-Flooder
- Flooder
- HackTool
- Hoax
- IM-Flooder
- SMS-Flooder
- Spoofers
- VirTool

PUPs

AdWare

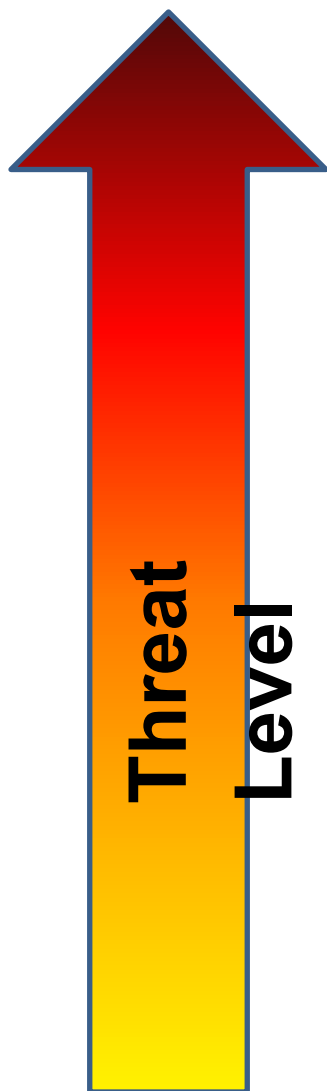
PornWare

- Porn-Dialer
- Porn-Downloader
- Porn-Tool

RiskWare

- Client-IRC
- Client-P2P
- Client-SMTP
- Dialer
- Downloader
- FraudTool
- Monitor
- NetTool
- PSWTool
- RemoteAdmin
- RiskTool
- Server-FTP
- Server-Proxy
- Server-Telnet
- Server-Web
- WebToolbar

- Prefix
- Behaviour
- Platform
- Name
- Variant



- Viruses and Worms
- Trojan Programs
- Malicious Tools

- Вредоносная программа, распространяется через локальную сеть и при помощи съемных носителей информации. Программа является динамической библиотекой Windows (PE DLL-файл).
- Встречается впервые. Похожих вредоносных объектов не найдено.
- В программе встречаются ссылки :
 - <http://www.getmyip.org>
 - <http://getmyip.co.uk>
 - <http://checkip.dyndns.org>

Net-Worm.Win32.Kido.a

- Программа, которая без ведома пользователя скачивает на компьютер другое программное обеспечение и запускает его на исполнение. Программа является приложением Windows (PE EXE-файл). Имеет размер 79360 байт. Написана на C++.
- Есть две аналогичные разновидности этой вредоносной программы

Trojan-Downloader.Win32.Braidupdate.c

- Программа для смартфонов, работающих под управлением ОС Symbian. Представляет собой установочный SIS-архив. Размер вирусного файла составляет 121723 байта.
- Основной деструктивный функционал вредоносной программы — отправка SMS-сообщений на специальные платные номера.
- SMS посылаются без ведома пользователя и через установленные промежутки времени.
- Собственной процедуры распространения не имеет.
- Есть одна аналогичная разновидность этой вредоносной программы

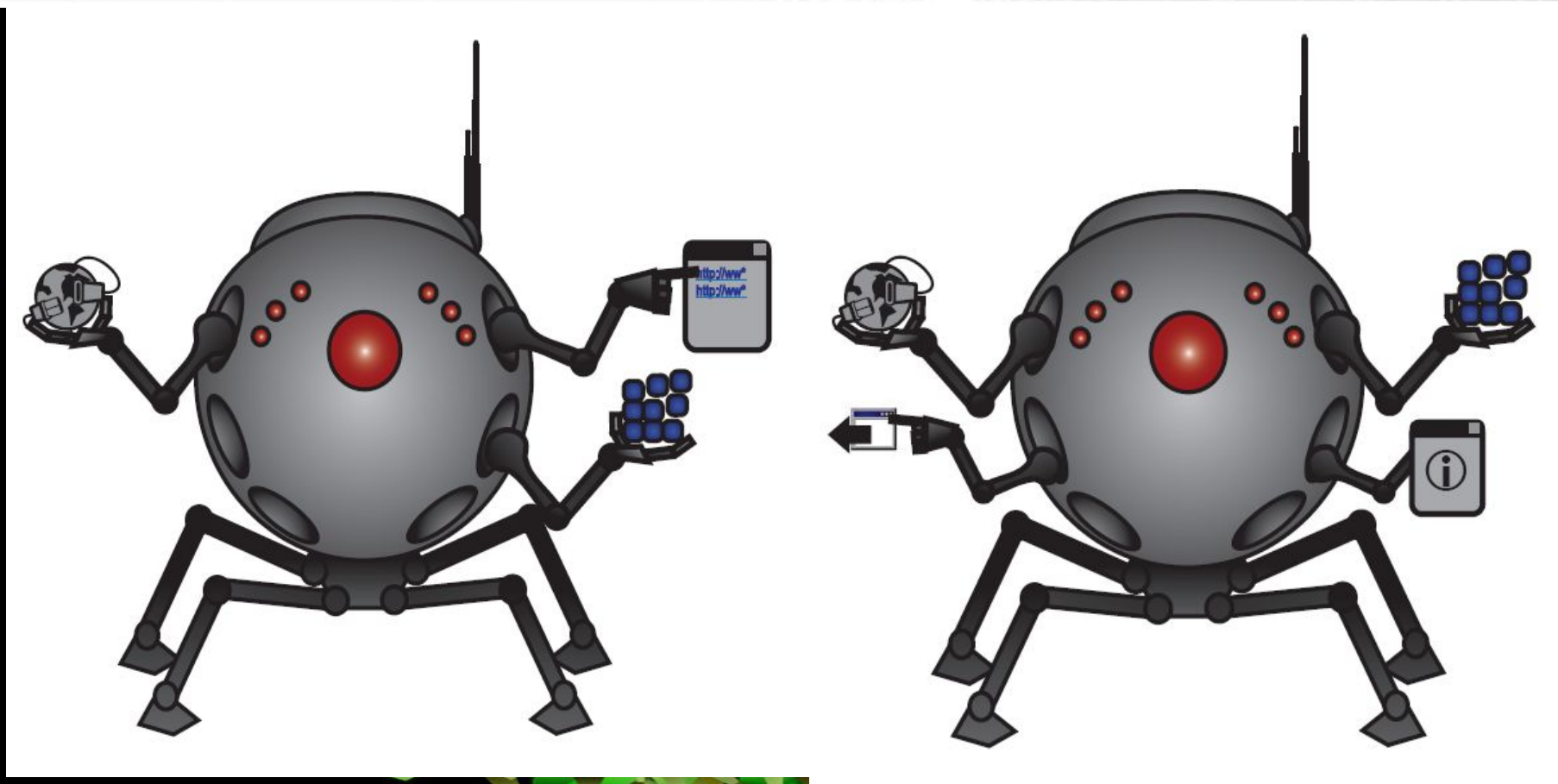
Trojan-SMS.SymbOS.Viver.b

The background is a light gray gradient with a faint grid of white lines. In the lower half, there are several vertical white bars of varying heights, resembling a bar chart or data visualization.

Будущее ?

Завтра начинается сегодня

- Anti-Virtual Machine
- Anti-Emulation, Неполная эмуляция
- Работает на специфической ОС (Windows XP с испанским интерфейсом)
- Действия пользователя
- Один маршрут исполнения



- Нужна ли классификация? – Да!
- Что дает нам классификация? – Новые знания!
- Авто классификация – хорошее подспорье в работе аналитика
- Есть над чем работать?
 - Разработка
 - Коммуникации, создание единого подхода

Спасибо! Вопросы?