Презентация подготовлена для конкурса «Интернешка» http://interneshka.org на тему: «Компьютерные вирусы. Антивирусные программы».

Работу выполнил Таран Андрей ученик 8 «А» класса

Компьютерный вирус

Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Принято разделять вирусы:

1)по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);

2)файловые вирусы делят по механизму заражения:

а)паразитирующие добавляют себя в исполняемый файл,

б)перезаписывающие невосстановимо портят заражённый файл,

в) «спутники» идут отдельным файлом.

3)по поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unix, Linux);

4)по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);

5)по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);

6)по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.)

История создания вирусов

- Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. С 1961 года известны рабочие примеры таких программ.
- Первыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году. Зимой 1984 года появились первые антивирусные утилиты — CHK4BOMB и BOMBSQAD авторства Энди Хопкинса. В начале 1985 года Ги Вонг написал программу DPROTECT — первый резидентный антивирус.
- Первые вирусные эпидемии относятся к 1986—1989 годам: Brain.A (распространялся в загрузочных секторах дискет, вызвал крупнейшую эпидемию), Jerusalem (проявился в пятницу 13 мая 1988 года, уничтожая программы при их запуске), червь Морриса (свыше 6200 компьютеров, большинство сетей вышло из строя на срок до пяти суток), DATACRIME (около 100 тысяч зараженных ПЭВМ только в Нидерландах).
- Тогда же оформились основные классы двоичных вирусов: сетевые черви (червь Морриса, 1987), «троянские кони» (AIDS, 1989), полиморфные вирусы (Chameleon, 1990), стелс-вирусы (Frodo, Whale, 2-я половина 1990).
- Параллельно оформляются организованные движения как про-, так и антивирусной направленности: в 1990 году появляются специализированная BBS Virus Exchange, «Маленькая чёрная книжка о компьютерных вирусах» Марка Людвига, первый коммерческий антивирус Symantec Norton AntiVirus.

Антивирусная программа

Антивирусная программа (**антивирус**) — программа для обнаружения и лечения программ, заражённых компьютерным вирусом, а также для предотвращения заражения вирусом.

Классификация антивирусных программ

- По функционалу продуктов:
  - Антивирусные продукты (продукты, обеспечивающие только антивирусную защиту)
  - Комбинированные продукты (продукты, обеспечивающие не только защиту от вредоносных программ, но и фильтрацию спама, шифрование и резервное копирование данных и другие функции)
- По целевым платформам:
  - Антивирусные продукты для ОС семейства Windows
  - Антивирусные продукты для ОС семейства *NIX (к данному семейству относятся ОС BSD, Linux и др.)
  - Антивирусные продукты для ОС семейства MacOS
  - Антивирусные продукты для мобильных платформ (Windows Mobile, Symbian, iOS, BlackBerry, Android, Windows Phone 7 и др.)
- Антивирусные продукты для корпоративных пользователей можно также классифицировать по объектам защиты:
  - Антивирусные продукты для защиты рабочих станций
  - Антивирусные продукты для защиты файловых и терминальных серверов
  - Антивирусные продукты для защиты почтовых и Интернет-шлюзов
  - Антивирусные продукты для защиты серверов виртуализации
  - и т.д.
- По используемым технологиям антивирусной защиты:
  - Классические антивирусные продукты (продукты , применяющие только сигнатурный метод детектирования, продукты, применяющие только проактивные технологии антивирусной защиты);
  - Комбинированные продукты (продукты, применяющие как сигнатурные методы

Методы обнаружения вирусов антивирусными программами

Антивирусное программное обеспечение обычно использует два отличных друг от друга метода для выполнения своих задач:

- Сканирование файлов для поиска известных вирусов, соответствующих определению в антивирусных базах
- Обнаружение подозрительного поведения любой из программ, похожего на поведение заражённой программы.

Антивирус может по запросу выполнить одно из следующих действий:

- Удалить инфицированный файл.
- Заблокировать доступ к инфицированному файлу.
- Отправить файл в карантин (то есть сделать его недоступным для выполнения, с целью недопущения дальнейшего распространения вируса).
- Попытаться восстановить файл, удалив сам вирус из тела файла.
- В случае невозможности лечения/удаления, выполнить эту процедуру при перезагрузке

Наиболее распространённые антивирусные программы

Интересные факты

В 2009 началось активное распространение лжеантивирусов — программного обеспечения, не являющегося антивирусным (то есть не имеющего реальной функциональности для противодействия вредоносным программам), но выдающим себя за таковое. По сути, лжеантивирусы могут являться как программами для обмана пользователей и получения прибыли в виде платежей за «лечение системы от вирусов», так и обычным вредоносным программным обеспечением. В настоящий момент это распространение приостановлено.

Специальные антивирусы

В ноябре 2014 года международная правозащитная организация Amnesty International выпустила антивирусную программу Detect, предназначенную для выявления вредоносного ПО, распространяемого государственными учреждениями для слежки за гражданскими активистами и политическими оппонентами. Антивирус выполняет более глубокое сканирование жёсткого диска, нежели обычные антивирусы

Антивирусные компании и программы

AOL® Virus Protection в составе AOL Safety and Security Center

ActiveVirusShield от AOL (на базе KAV 6, бесплатная)

AhnLab

Aladdin Knowledge Systems

ALWIL Software (avast!) из Чехии (бесплатная и платная версии)

ArcaVir из Польши

AVZ из России (бесплатная)

Avira из Германии (есть бесплатная версия Classic)

Authentium из Великобритании

BitDefender из Румынии

BullGuard из Дании

Computer Associates из США

Comodo Group из США

ClamAV — Лицензия GPL — бесплатный с открытым исходными кодами программы

ClamWin — ClamAV для ОС Windows

Dr.Web из России

Eset NOD32 из Словакии

Fortinet

Frisk Software из Исландии

ВирусБлокАда (VBA32) из Беларуси

VirusBuster из Венгрии

ZoneAlarm AntiVirus (из Zone Labs)

VirusBuster из Венгрии

F-Secure из Финляндии

GeCAD из Румынии (Microsoft купил компанию в 2003)

GFI Software

GriSoft (AVG) из Чехии (бесплатная и платная версии)

Hauri

H+BEDV из Германии

Kaspersky из России

McAfee из США

MicroWorld Technologies из Индии

NuWave Software из Украины

MKS из Польши

Norman из Норвегии

NOD32

Outpost из России

Panda Software из Испании

Quick Heal AntiVirus из Индии

Rising

ROSE SWE

Sophos из Великобритании

Stiller Research

Sybari Software (Microsoft купил компанию в начале 2005)

Symantec из США или Великобритания

Trojan Hunter

Trend Micro из Японии (номинально Тайвань-США)

Украинский Национальный Антивирус из Украины

ВирусБлокАда (VBA32) из Беларуси

Спасибо за просмотр