Компьютерные вирусы. Антивирусные программы.

Работу выполнила ученица г.Клин школы №17, ,,8А" класса
Кондрашова Алина

"Презентация подготовлена для конкурса
"Интернешка" http://interneshka.org/".

Что такое 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.

Начало исходного кода вируса для MS-DOS на языке ассемблера

```
text    segment   'code'
        assume cs:text,ds:text
        org     100h    main

main    proc
        jmp     VirStart            ;Переход на вирус
        db      'A'                 ;Маркер заражённости
        mov     ax,4C00h            ;Штатное завершение
        int     21h

VirStart:
        call    $+3                 ;Определение адреса
FindIP: pop     bp                  ;начала вируса
        sub     bp,offset FindIP

        mov     di,100h             ;Восстановление
        lea     si,[bp+OldBytes]    ;оригинального начала
        movsw                       ;заражённого файла
        movsw

        mov     ax,2524h            ;Переопределение int 24h
        lea     dx,[bp+New_24h]
        int     21h

        call    FindVictimFiles     ;Подпрограмма поиска и заражения
                                    ;жертв

        mov     ah,1Ah              ;Восстановление int 24h
        mov     dx,80h
        int     21h
```

История компьютерных вирусов.

- 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 Энд Хопкинса (англ. *Andy Hopkins*). В начале 1985 года Ги Вонг (англ. *Gee Wong*) написал программу DPROTECT — первый резидентный антивирус. В 1992 году появились первый конструктор вирусов для PC — VCL (для Amiga конструкторы существовали и ранее), а также готовые полиморфные модули (MtE, DAME и TPE) и модули шифрования для встраивания в новые вирусы. В 1996 году появился первый вирус для Windows 95 — Win95.Boza, а в декабре того же года — первый резидентный вирус для неё — Win95.Punch.

Формальное определение

- Формально вирус определён Фредом Коэном со ссылкой на машину Тьюринга следующим образом:
- $M : (S_M, I_M, O_M : S_M \times I_M > I_M, N_M : S_M \times I_M > S_M, D_M : S_M \times I_M > d)$
- $\forall C_M \ \forall t \ \forall j: S_M(t) = S_{Mo} \wedge P_M(t) = j \wedge \{C_M(t, j) \dots C_M(t, j + |v| - 1)\} = v \Rightarrow \exists v' \exists j' \exists t' \exists t'': t < t'' < t' \wedge \{j' \dots j' + |v'|\} \cap \{j \dots j + |v|\} = \varnothing \wedge \{C_M(t', j') \dots C_M(t', j' + |v'| - 1)\} = v' \wedge P_M(t'') \in \{ j' \dots j' + |v'| - 1 \}$

Классификация

- Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности.
  В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:
- по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);
- файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.
- по поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unix, Linux);
- по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);
- по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);
- по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.)

Механизм

- Вирусы распространяются, копируя свое тело и обеспечивая его последующее исполнение: внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды — например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплоитом, использующим уязвимость.

Каналы

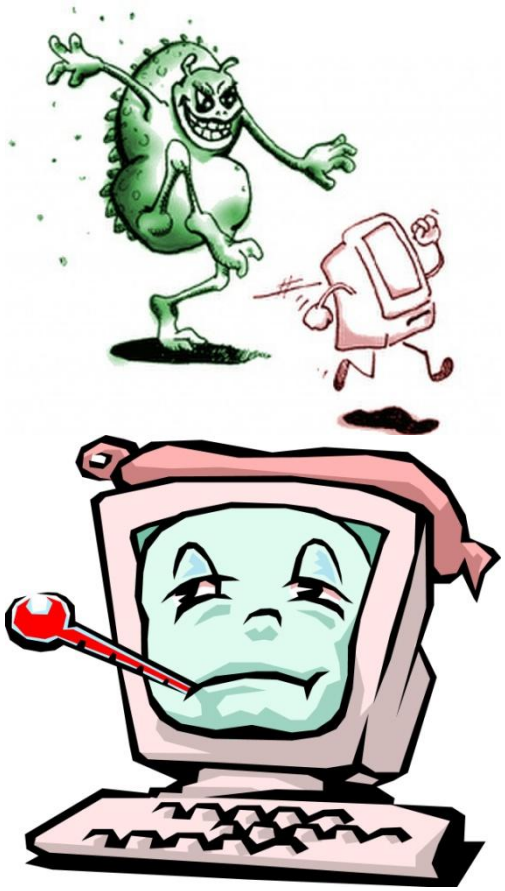
- Дискеты
  Флеш-накопители
  Электронная почта
  Системы обмена мгновенными сообщениями
  Веб-страницы
  Интернет и локальные сети

Профилактика и лечение

- Не работать под привилегированными учётными записями без крайней необходимости. (Учётная запись администратора в Windows)
- Не запускать незнакомые программы из сомнительных источников.
- Стараться блокировать возможность несанкционированного изменения системных файлов.
- Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
- Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
- Пользоваться только доверенными дистрибутивами.
- Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.
- Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

Экономика

- Некоторые производители антивирусов утвержд ают, что сейчас создание вирусов превратилось из одиночного хулиганского занятия в серьёзный бизнес, имеющий тесные связи с бизнесом спама и другими видами противозаконной деятельности.
- Также называются миллионные и даже миллиардные суммы ущерба от действий вирусов и червей. К подобным утверждениям и оценкам следует относиться осторожно: суммы ущерба по оценкам различных аналитиков различаются (иногда на три-четыре порядка), а методики подсчёта не приводятся.



Ссылки

- https://ru.wikipedia.org/wiki/Компьютерный_вирус
  https://yandex.ru/images/search?text=компьютерный%20вирус&stype=image&lr=10733&noreask=1&source=wiz

Спасибо за внимание!