Компьютерные вирусы 1

Общая информация о вирусах и антивирусах

• **Lionel S. Penrose** в 1959 г. – двумерная модель саморегулируемых механических структур.

Модель Пенроса реализована в машинном коде IBM 550 Шталем (L.G. Stahl).

•60 – 70 гг. XX в. Появление аналога современных вирусов - программа *Pervading Animal* - для компьютера Univac 1108 (типаmainframe).

Фактически первый вирус для исполнительных файлов. Назначение – предотвращение повторных инфекций файлов.

•Первый европейский студент Jürgen Kraus. В1980 г. в Дортмундском ун-те (RFN) – дипломная работа „*Selbstreproduktion bei Programmen*”.

•1983 г. в ун-те Lehigh (Пенсильвания, USA) Cohen –ряд экспериментов с саморепликующимися кодами для ОС VAX и Unix.

5 генераций вирусов:

1– простые,

2– «самоузнаваемые»,

3– «скрывающиеся»,

4– «вооруженные»,

5– изменяющие свойства.

Важнейшие даты в истории антивирусов 3

- **1988** Появление антивирусных фирм.

IBM инфицирована вирусом Cascade и начала исследования по борьбе с вир. в High Integrity Computing Laboratory (Yorktown).

Фирма S&S (Англия) – первый семинар .

S&S создает первый антивирус: *Anti Virus Toolkit*.

Первые стандарты антивирусов. Создание в США CERT (ang. Computer Emergency Response Team) – группа экспертов для антивир защиты в сетях DARPA.

- **1989** В Англии - Computer Threat Research Association (COTRA) – английский аналог CERT.

В Англии – создание бюллетеня *Virus Bulletin IBM* – представил - *Virscan* для MS-DOS. Сканер для детекции 28 вирусов.

Появление нового сканера *McAfee* – идентифицирует 44 вируса

- .**1990** для **н**овой технологии создания вируса – полиморфизма – использования сигнатур для обнаружения в. - неэффективно . **5**

В Гамбурге создан EICAR (ang. European Institute for Computer Antivirus Research) – объединение создателей антивирусов.

Фирма Symantec (создана в 1982) выпускает на рынок *Norton AntiVirus*.

- **1991** создание New Virus Naming Convention – новый стандарт «антивирусов». Борьба с вирусами ведется на основе *дизассемблирования* кодов.
- **1993** Создание Wild List Organization International и Wild List – списки существующих вирусов (ang. wild list)

Создание техники обнаружения полиформных в. - на основе технологии «эмуляции».

.....

Типы атак вирусов

- А. на доступ:
  - Удаление файлов,
  - Измен-е ф.,
  - Шифрование ф., катологов и т.д.,
  - Блокировка запуска системных ф..
- А. на интегральность:
  - Повреждение системных ф., стартового сектора д., таблицы FAT;
  - Модификация ф. с данными, в БД,
  - Повреждение исполнительных ф.
- А. на конфиденциальность:
  - Перехват паролей,
  - Перехват конфид данных, (PIN кодов и др.)

Термин «компьютерный вирус»

- **Появился в** 1983 г. в USA, Frederick Cohen
- Определение «к. в.» по dr Frederick Cohen: *“Программа, которая может инфицировать другую программу посредством такой ее модификации , чтобы она содержала ее копию и которая способна к эволюции*
- Соврем.: **Компьютерный вирус** — разновидность компьютерной программы, отличительной особенностью которой является **способность к размножению** (саморепликация). Вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру.

```
1.  Program wirus:
2.  {
3.  1234567;
4.  Подпрограмма инфицируй_исполнительная:=
5.   {
6.  Петля:файл = выбери_исполнительн_файл;
7.     If первая_строка_файла == 1234567 тогда
8.     Goto Петля;
9.  Присоедини_вирус_к_файлу;
10.  }
11. Подпрограмма уничтожь:=
12.   {
13.  //процедуры_уничтожающие_систему
14.  }
```

```
15 Подпрограмма условие_деструкции:=
16 {
17 If условие_деструкции Then
18     Return TRUE;
19  }
20 Главная_Подпрограмма:=
21 {
22  инфицируй_исполнительная;
23 If условие_инфекции Then
24   уничтожь;
25   Goto Next;
26   }
27  Next:
28  }
```

Блоки кода:

Инфекция – определение подпрограммы *инфицируй_исполнительная* (строки: 4 – 10);

Деструкция – пределение подпрограммы *уничтожь* (строки: 11 – 14) ; проверка условия процедуды деструкции - определение подпрограммы *условие_деструкции* (строки: Infe15 – 19).

- Инфекция начинается поиском и началом редакции файла, или другого эл-та системы (np., стартового сектора) – строка 6. Может быть реализован петлей (как в примере).

Условие начала инфекции (7).

- Строки 22 – 24 исполнение деструктивных действий.

Строка 25 – переход к *Next* – это может быть также переход к контролю носителя.

Функциональные блоки современного вируса: 11

- Механизм **распространения**,
- **Механизм инфекции**,
- Механизм **репликации**,
- **Механизм деструкции**,
- Механизм(ы) **дополнительный** (-е).

Систематизация вирусов

В. можно классифицировать по:

- отношению к аппаратной платформе:
  - В. не зависящие от апп.
  - В. зависящие от апп.
- отношению с ОС:
  - В. не зависящие от ОС.
  - В. зависящие от ОС.
- способу распростр-я.:
  - В. с непосредственным распр.,
  - В. с опосредованнымм распр.

Наибольшая группа в. Исполнительных ф., делятся на:

- дописываемые (ang. overwriting),
- паразитические (ang. parasitic),
- присоединяемые (ang. link virus),
- сопутствующие(ang. companion).

Паразитические вирусы

- Пример – в. Исполнительных ф. – запускаются непосредственно ОС
- Способ инфицирования:

  Конца ф., (а – на рис.)

  Начала ф., (в – на рис.)

  Внутри ф.. (с – на рис.)

Инфекция состоит во вмешательстве в структуру ф.:

- Инфекция конца ф. (a) – самый простой способ инфекции; Адрес начала исполняемого кода – начало вируса.
- B. Может размест-ся в заголовке либо в первом сегм. (**b**),
- Наиболее сложный метод (**c**) – в. разм-ся в неиспользуемых секторах ф-ла

- Семейство 32-битных ОС использует для исп. ф-лов специальный формат – Portable Executable (PE): файлы EXE, DLL, SYS

- Заглавие PE, таблица секции , отдельные секции
- Перед инфекцией вирус должен идентифицировать ф. (это PE? : две первые строки файла - 'MZ' ?)
- Метод инфиц-я PE – измен-е содержания заглавия: он может быть перемещен в иную область. Секция может быть модифицирована либо сжата.
- Вирус м.б. записан в свободные места файла.

Макровирусы

- В. не зависит от типа ОС.
- **Макровирусы** (ang. *macro viruses*) инфицируют файлы, содержащие определение makro, np. док-ты **MS Word**, **MS Excel**, itd.
- Makro, - ряд инструкций на языке VBA;
- Почти все Makro можно вставить в док-ты (**.DOC*), шаблоны (**.DOT*) и шаблоны глабальные (*NORMAL.DOT*)

Анализ техник защиты от в.

- Нет алгоритмов, позволяющих в 100% случаев отличить вирус от невируса
- 3 фундаментальных способа обнаружения в.:

Техника сканирования.

Техника мониторинга.

Техника контроля интегральности

- Из этого следуют 3 типа антивирусов:

Сканеры,

Мониторы,

Контролеры интегральности.

Техника сканирования сигнатур в.

- Термин **skaner** здесь имеет лексический смысл – это средство анализа совпадающих строк данных.
- Сканер анализирует PE, старт. сектор, память – поиск характеристических строк шестнадцатеричных знаков (известных в.)
- Требует выполнения операций:

Поиск в.,

Генерация сообщения.

- Сканер состоит из:

Машина поска (ang. searching engine),

База известных в. (**сигнатур в. – уникальных последовательностей шестнадцатеричных данных**).

- Хорошая сигнатура д.соотв-ть двум требованиям:

Отличаться от остальных с.,

Отличаться от последовательность в неинфицированных ф-лах.

- Примеры с.:

Paulus.1804:

B9 D5 00 8B DE ?? ?? 27 06 53 ?? ?? 07 86 CA ?? ?? 86 CA 2E 88 07 4A ??

V.974:

9C 80 FC AA 75 04 B4 BB 9D CF 80 FC 4B 74 0B 80 FC AB 74 06 9D 2E FF 2E

Мониторы

•**Monitor** – резидентная программа, анализирующая выполнение ОС заданных функций и предназначенная для анализа:

Модификации PE,

Размещения программ в операт. памяти,

Перехвата прерываний,

Доступа к диску і tp.

• Характеристики мониторов:

«Принимают решение» в результате обнаружения подозрительных операций: изменение таблицы прерываний, запись информации в стартовый диск и др

Контроль интегральности

- **Основан на подсчете и анализе контрольных сумм (CRC)** исп. Ф. и хранении их в памяти.
- Использует алгоритмы шифрования DES, MD4, MD5, RSA, (минимум – избыточное кодирование)
- Контрольная сумма хранится внутри прогр. либо отдельно
- Алгоритмы подсчета сумм контр.:

Простые,

На основе циклических кодов (ang.cyclic redundance checks - CRC,

В зашифрованной форме.

В последнее время

Антивирусные программы делятся на:

программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры, программы-вакцины.

Программы-детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение.

Программы-доктора (фаги), не только находят зараженные вирусами файлы, но и "лечат" их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние.

Программы-ревизоры - самые надежные средства защиты. Запоминают исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем сравнивают текущее состояние с исходным.

Программы-ревизоры имеют развитые алгоритмы, обнаруживают стелс-вирусы, могут отличить изменения версии проверяемой программы от изменений, внесенных вирусом.

Программы-фильтры (сторожа) - небольшие резидентные программы для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

. попытки коррекции файлов с расширениями COM и EXE;

. изменение атрибутов файлов;

. прямая запись на диск по абсолютному адресу;

. запись в загрузочные сектора диска.

. загрузка резидентной программы.

Firewalls

Список лучших бесплатных файерволов :

Gomodo Firewall (http://www.personalfirewall.comodo.com),

Online Armor Free (http://www.tallemu.com/onlme_armor_free.html),

Jetico Personal Firewall Freeware (http://www.jetico.com/jpfwall.exe),

ZoneAlarm Free Firewall (http://www.zonealafm.com),

Sygate Personal Firewall (http://www.tucows.com/preview/213160),

R-Firewall (http://vvww.r-ircwall.com/R_Firewall_Download.shtml),

PC Tools Firewall Plus (http://www.pctools.com/ru/firewaW),

Safety.Net (http://www.netveda.com/downioads/index.htm).