RuxCon 2004

Reverse Engineering for Malware Analysis

by: Peter Taylor

email: nevar<insert at symbol>feline<no space>menace<full stop>com

RuxCon 2004

Introduction

- What is "Malware"
  - Software with malicious intent
  - Software with sinister motives

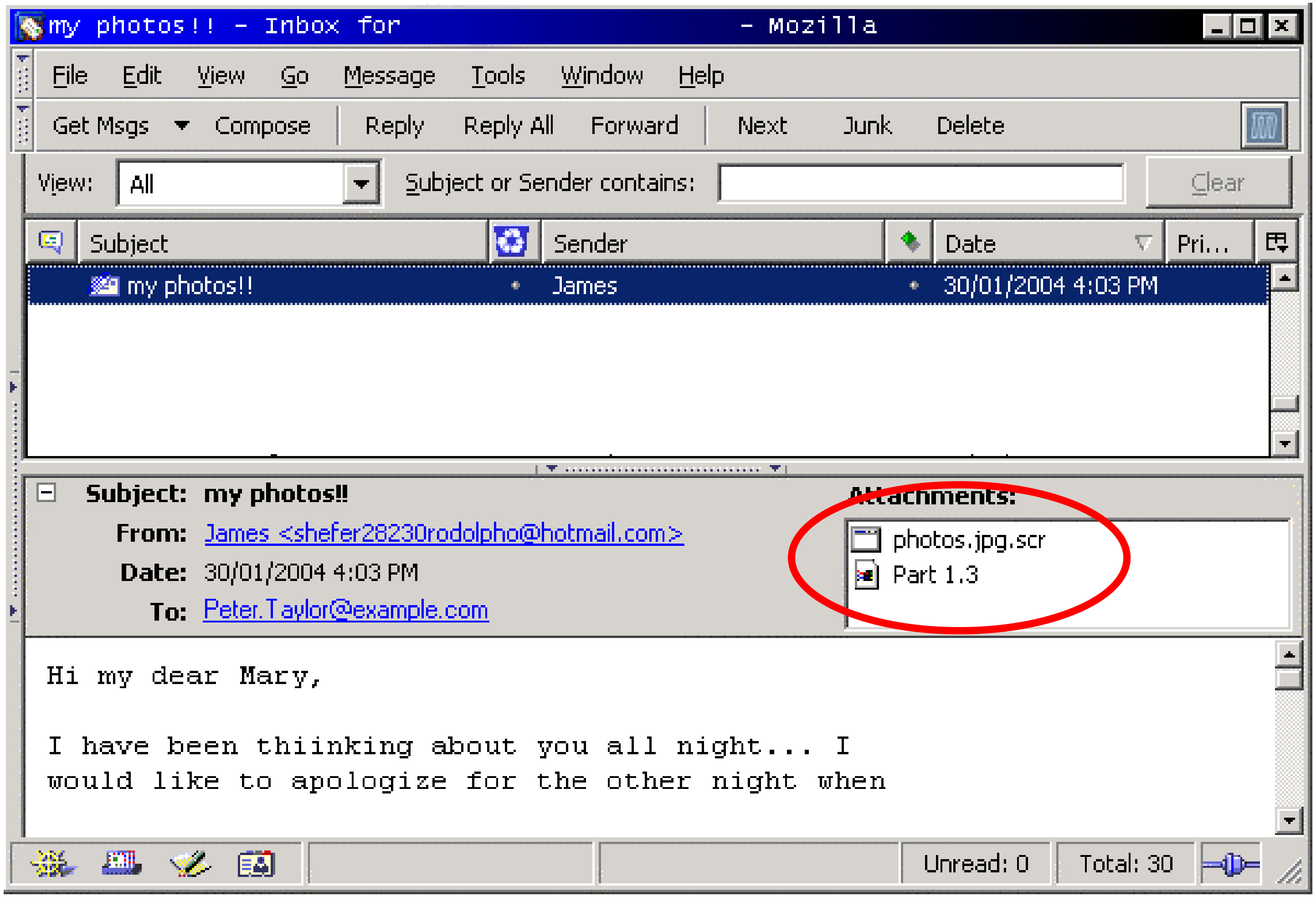
Introduction

- What is "Malware"
  - Software with malicious intent
  - Software with sinister motives
- Is there a need for specialized R.E. when dealing with malware

R.E. and Malware

- Time is of the essence
- No complex algorithms or data-structures to reverse engineer
- A small subset of system functions work together to exhibit malicious behaviour
- Lack of imagination and release of malware source leads to rampant function re-use
- Code to intricately manipulate executable file headers has few reason to appear in notepad.exe

Contracting Malware - Did you get my email ?


my photos!! - Inbox for - Mozilla
File Edit View Go Message Tools Window Help
Get Msgs Compose Reply Reply All Forward Next Junk Delete
View: All
Subject or Sender contains:
Clear
Subject
Sender
Date
Pri...
Unread: 0
Total: 30

my photos!! James 30/01/2004 4:03 PM

Subject: **my photos!!**

From: James <shefer28230rodolpho@hotmail.com>

Date: 30/01/2004 4:03 PM

To: Peter.Taylor@example.com

Attachments:

photos.jpg.scr

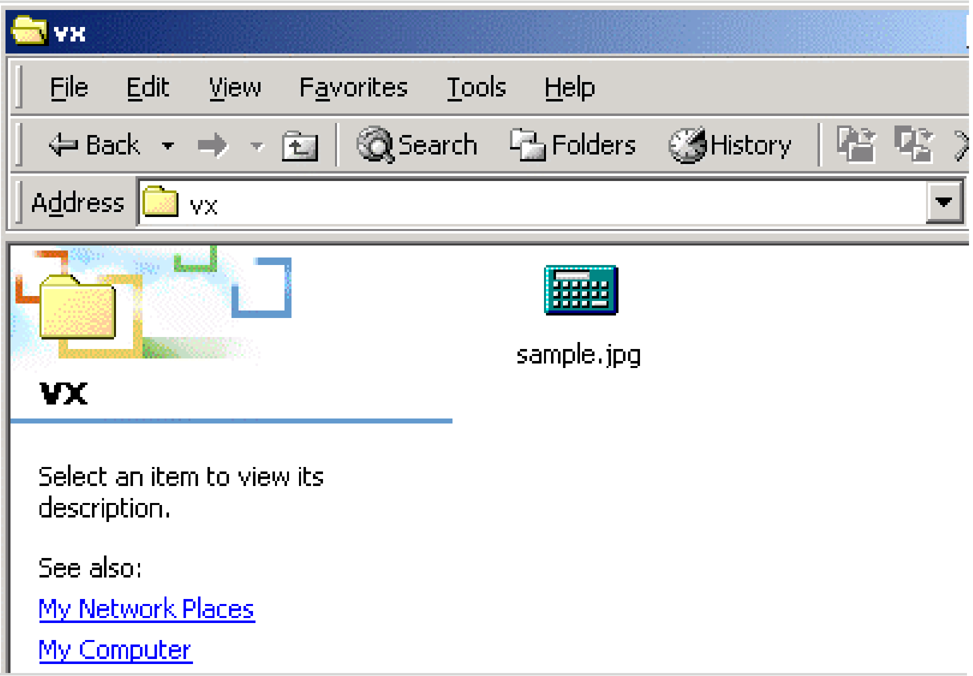
Part 1.3

```
Hi my dear Mary,

I have been thiinking about you all night... I
would like to apologize for the other night when
```

Explorer Trickery

- Too many smarts spoil the Puter. Sometimes software tries to be too clever and malware authors like to exploit this fact


vx
File Edit View Favorites Tools Help
Back Search Folders History
Address

Address: vx

vx

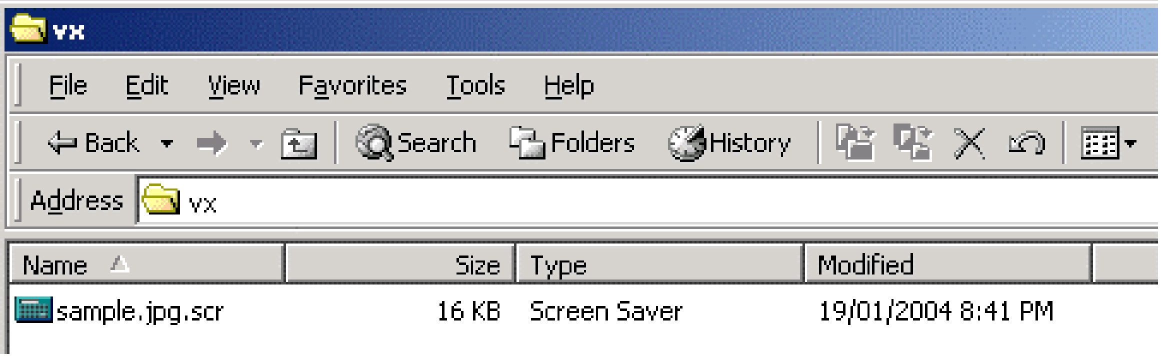
Select an item to view its description.

See also:

My Network Places

My Computer

sample.jpg

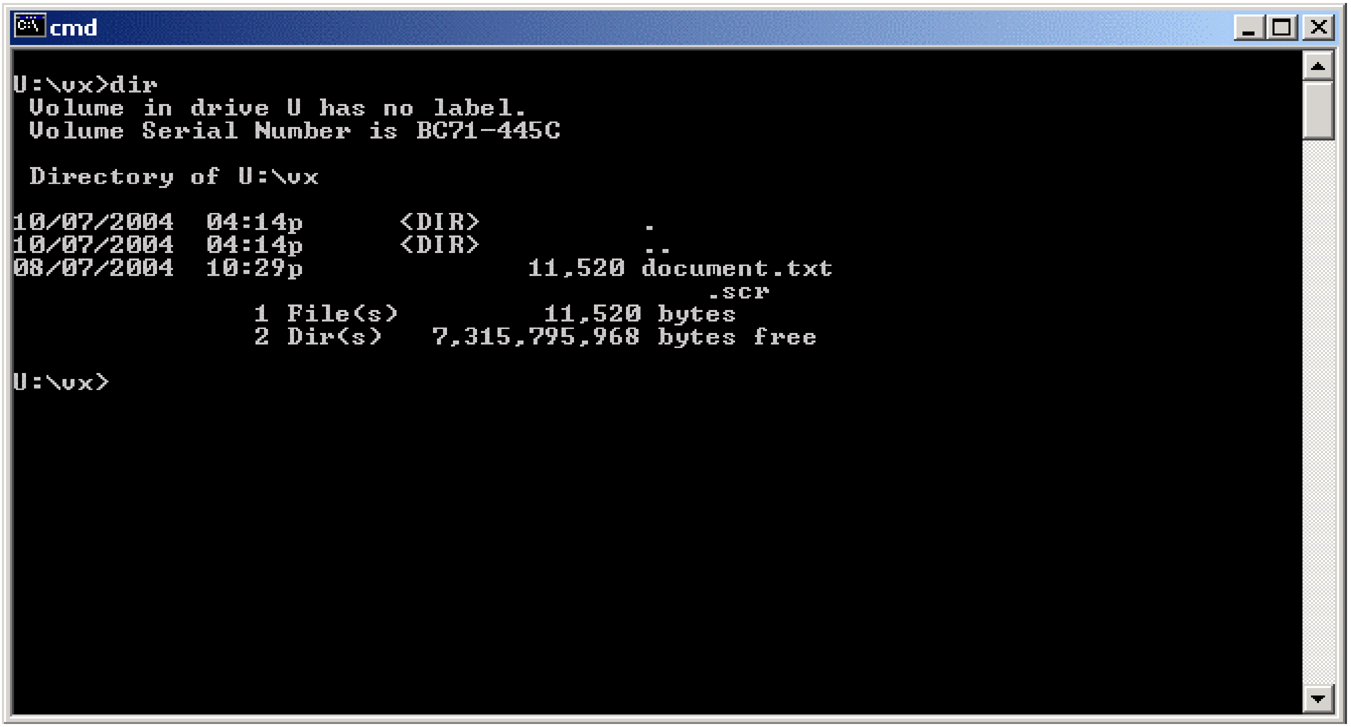

vx
File Edit View Favorites Tools Help
Back Search Folders History
Address

Address: vx

Name	Size	Type	Modified
sample.jpg.scr	16 KB	Screen Saver	19/01/2004 8:41 PM

Cursory Analysis

'dir' yields much to the keen observer



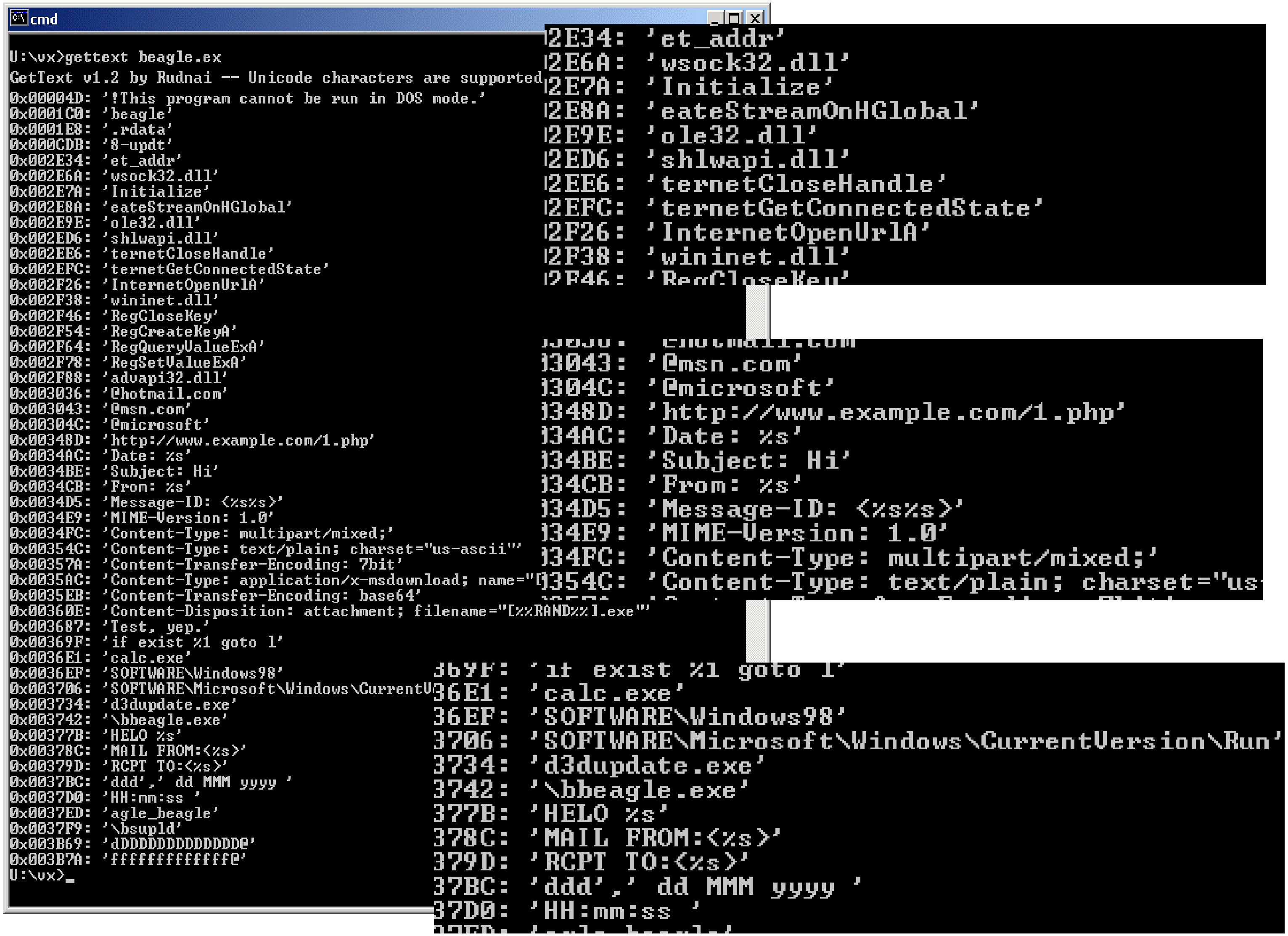
```
U:\vx>dir
 Volume in drive U has no label.
 Volume Serial Number is BC71-445C

 Directory of U:\vx

10/07/2004  04:14p      <DIR>          .
10/07/2004  04:14p      <DIR>          ..
08/07/2004  10:29p              11,520 document.txt
                                           .scr
               1 File(s)         11,520 bytes
               2 Dir(s)   7,315,795,968 bytes free

U:\vx>
```

Mary had a little *beagle*...?



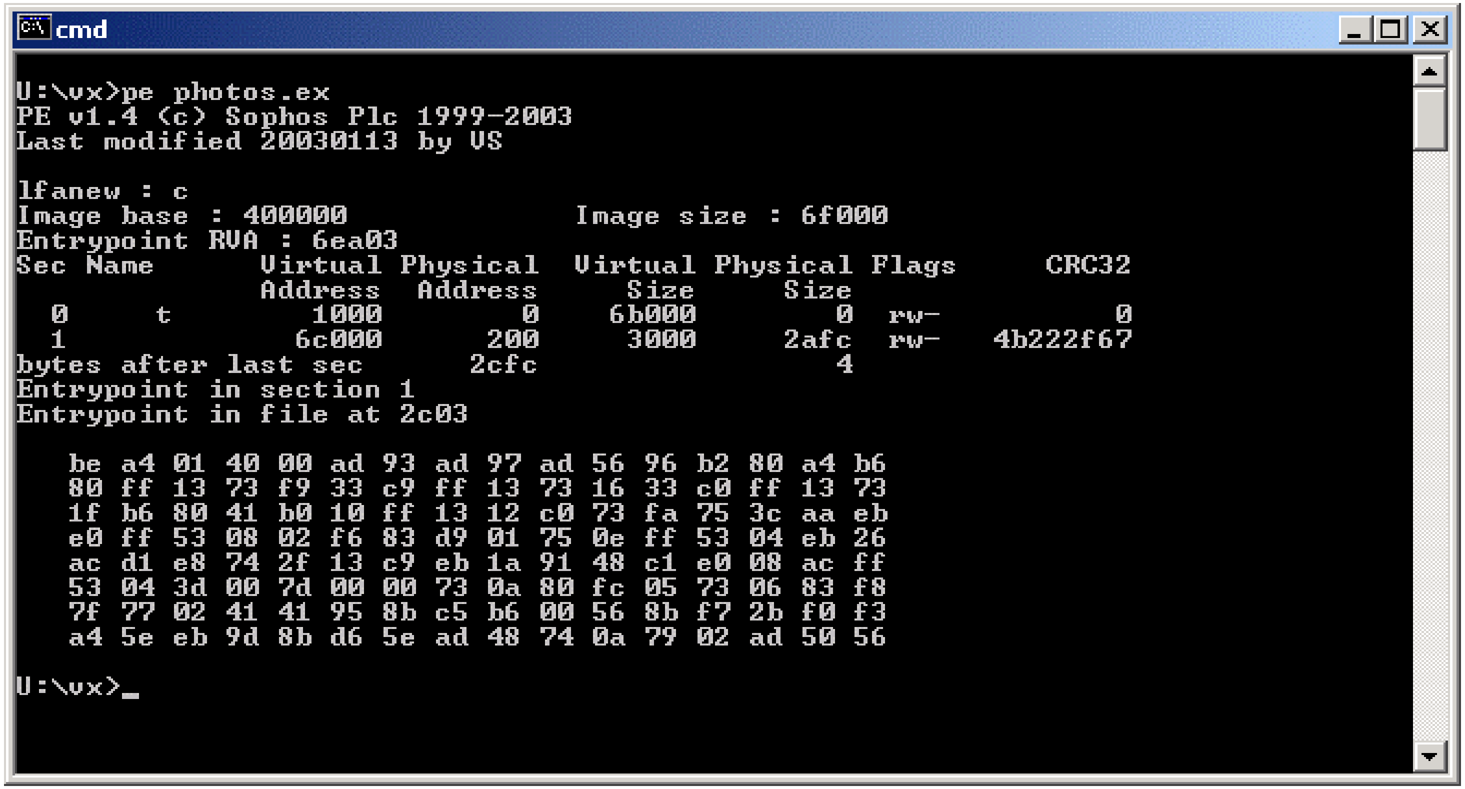
```
U:\vx>gettext beagle.ex
GetText v1.2 by Rudnai -- Unicode characters are supported
0x00004D: '!This program cannot be run in DOS mode.'
0x0001C0: 'beagle'
0x0001E8: '.rdata'
0x000CDB: '8-updt'
0x002E34: 'et_addr'
0x002E6A: 'wsock32.dll'
0x002E7A: 'Initialize'
0x002E8A: 'eateStreamOnHGlobal'
0x002E9E: 'ole32.dll'
0x002ED6: 'shlwapi.dll'
0x002EE6: 'ternetCloseHandle'
0x002EFC: 'ternetGetConnectedState'
0x002F26: 'InternetOpenUrlA'
0x002F38: 'wininet.dll'
0x002F46: 'RegCloseKey'
0x002F54: 'RegCreateKeyA'
0x002F64: 'RegQueryValueExA'
0x002F78: 'RegSetValueExA'
0x002F88: 'advapi32.dll'
0x003036: '@hotmail.com'
0x003043: '@msn.com'
0x00304C: '@microsoft'
0x00348D: 'http://www.example.com/1.php'
0x0034AC: 'Date: %s'
0x0034BE: 'Subject: Hi'
0x0034CB: 'From: %s'
0x0034D5: 'Message-ID: <%s%s>'
0x0034E9: 'MIME-Version: 1.0'
0x0034FC: 'Content-Type: multipart/mixed;'
0x00354C: 'Content-Type: text/plain; charset="us-ascii"'
0x00357A: 'Content-Transfer-Encoding: 7bit'
0x0035AC: 'Content-Type: application/x-msdownload; name="[
0x0035EB: 'Content-Transfer-Encoding: base64'
0x00360E: 'Content-Disposition: attachment; filename="[%%RAND%%].exe"'
0x003687: 'Test, yep.'
0x00369F: 'if exist %1 goto l'
0x0036E1: 'calc.exe'
0x0036EF: 'SOFTWARE\Windows98'
0x003706: 'SOFTWARE\Microsoft\Windows\CurrentV
0x003734: 'd3dupdate.exe'
0x003742: '\bbeagle.exe'
0x00377B: 'HELO %s'
0x00378C: 'MAIL FROM:<%s>'
0x00379D: 'RCPT TO:<%s>'
0x0037BC: 'ddd',' dd MMM yyyy '
0x0037D0: 'HH:mm:ss '
0x0037ED: 'agle_beagle'
0x0037F9: '\bsupld'
0x003B69: 'dDDDDDDDDDDDDD@'
0x003B7A: 'fffffffffffff@'
U:\vx>_
```

```
2E34: 'et_addr'
2E6A: 'wsock32.dll'
2E7A: 'Initialize'
2E8A: 'eateStreamOnHGlobal'
2E9E: 'ole32.dll'
2ED6: 'shlwapi.dll'
2EE6: 'ternetCloseHandle'
2EFC: 'ternetGetConnectedState'
2F26: 'InternetOpenUrlA'
2F38: 'wininet.dll'
2F46: 'RegCloseKey'
```

```
3036: '@hotmail.com'
3043: '@msn.com'
304C: '@microsoft'
348D: 'http://www.example.com/1.php'
34AC: 'Date: %s'
34BE: 'Subject: Hi'
34CB: 'From: %s'
34D5: 'Message-ID: <%s%s>'
34E9: 'MIME-Version: 1.0'
34FC: 'Content-Type: multipart/mixed;'
354C: 'Content-Type: text/plain; charset="us-
```

```
369F: 'if exist %1 goto l'
36E1: 'calc.exe'
36EF: 'SOFTWARE\Windows98'
3706: 'SOFTWARE\Microsoft\Windows\CurrentVersion\Run'
3734: 'd3dupdate.exe'
3742: '\bbeagle.exe'
377B: 'HELO %s'
378C: 'MAIL FROM:<%s>'
379D: 'RCPT TO:<%s>'
37BC: 'ddd',' dd MMM yyyy '
37D0: 'HH:mm:ss '
```

Section Dissection



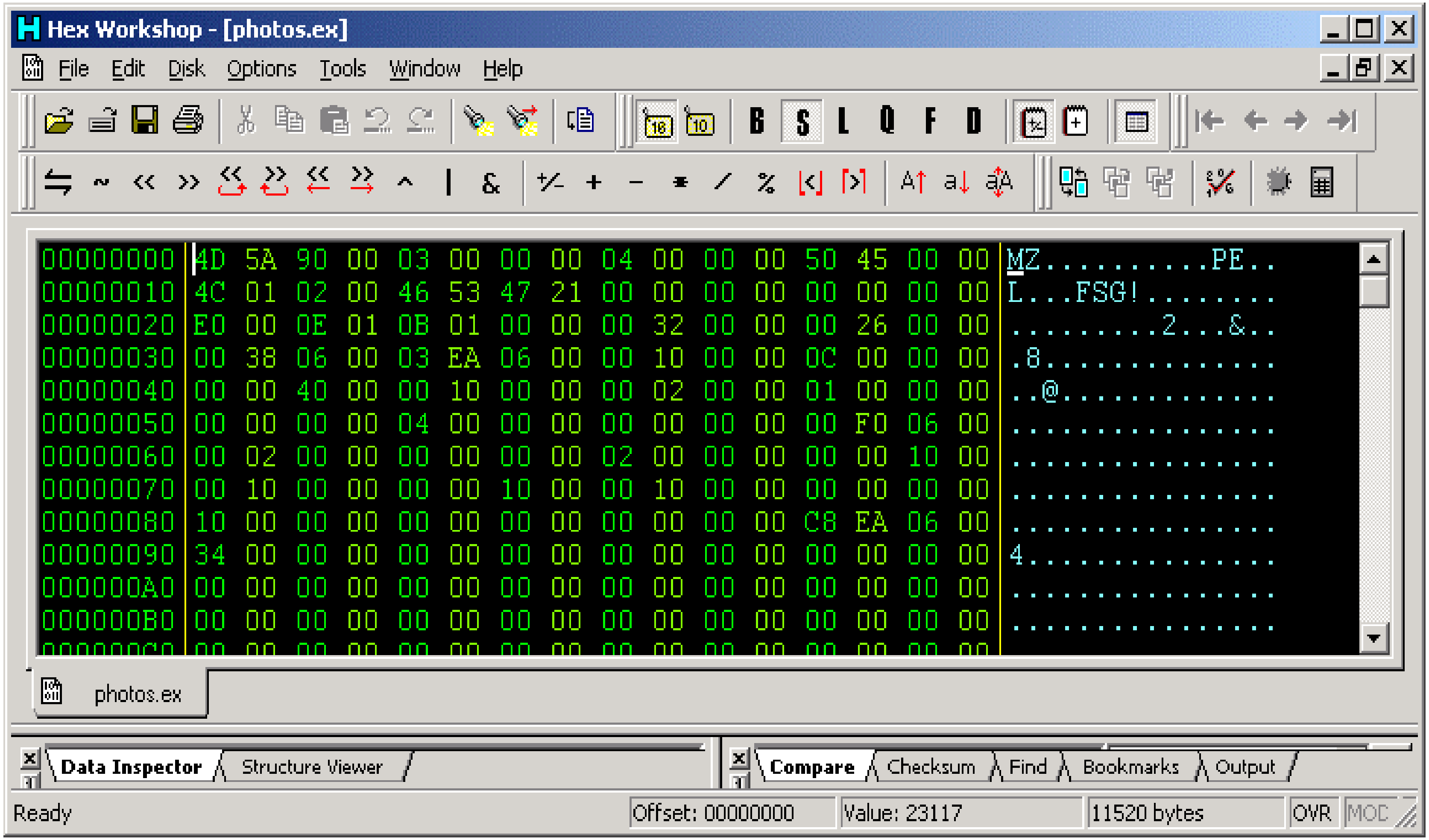
```
U:\vx>pe photos.ex
PE v1.4 (c) Sophos Plc 1999-2003
Last modified 20030113 by VS

lfanew : c
Image base : 400000             Image size : 6f000
Entrypoint RVA : 6ea03
Sec Name      Virtual Physical  Virtual Physical Flags     CRC32
              Address  Address     Size     Size
  0     t        1000        0    6b000        0  rw-            0
  1             6c000      200     3000     2afc  rw-     4b222f67
bytes after last sec      2cfc                 4
Entrypoint in section 1
Entrypoint in file at 2c03

   be a4 01 40 00 ad 93 ad 97 ad 56 96 b2 80 a4 b6
   80 ff 13 73 f9 33 c9 ff 13 73 16 33 c0 ff 13 73
   1f b6 80 41 b0 10 ff 13 12 c0 73 fa 75 3c aa eb
   e0 ff 53 08 02 f6 83 d9 01 75 0e ff 53 04 eb 26
   ac d1 e8 74 2f 13 c9 eb 1a 91 48 c1 e0 08 ac ff
   53 04 3d 00 7d 00 00 73 0a 80 fc 05 73 06 83 f8
   7f 77 02 41 41 95 8b c5 b6 00 56 8b f7 2b f0 f3
   a4 5e eb 9d 8b d6 5e ad 48 74 0a 79 02 ad 50 56

U:\vx>_
```

All this HEX is Byting me!



```
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 50 45 00 00 MZ..........PE..
00000010 4C 01 02 00 46 53 47 21 00 00 00 00 00 00 00 00 L...FSG!........
00000020 E0 00 0E 01 0B 01 00 00 00 32 00 00 00 26 00 00 .........2...&..
00000030 00 38 06 00 03 EA 06 00 00 10 00 00 0C 00 00 00 .8..............
00000040 00 00 40 00 00 10 00 00 00 02 00 00 01 00 00 00 ..@.............
00000050 00 00 00 00 04 00 00 00 00 00 00 00 00 F0 06 00 ................
00000060 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 ................
00000070 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 ................
00000080 10 00 00 00 00 00 00 00 00 00 00 00 C8 EA 06 00 ................
00000090 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4...............
000000A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000000B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000000C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Ready | Offset: 00000000 | Value: 23117 | 11520 bytes | OVR | MOD

Identifying some common file formats

```
00000000 55 45 73 44 42 41 6F 41 41 41 41 41 41 43 57 6C UEsDBAoAAAAAACWl
00000010 4D 7A 43 4B 6C 49 41 76 41 44 34 41 41 41 41 2B MzCKlIAvAD4AAAA+
00000020 41 41 41 4B 41 41 41 41 63 32 46 74 63 47 78 6C AAAKAAAAc2FtcGxl
00000030 4C 6D 56 34 5A 55 31 61 6B 41 41 44 0D 0A 41 41 LmV4ZU1akAAD..AA
00000040 41 41 42 41 41 41 41 50 2F 2F 41 41 43 34 41 41 AABAAAAP//AAC4AA
00000050 41 41 41 41 41 41 41 45 41 41 41 41 41 41 41 41 AAAAAAAEAAAAAAAA
```

Identifying some common file formats

```
00000000 50 4B 03 04 14 00 00 00 08 00 25 A5 33 30 8A 94 PK........%.30..
00000010 80 2F 34 1E 00 00 00 3E 00 00 0A 00 00 00 73 61 ./4....>......sa
00000020 6D 70 6C 65 2E 65 78 65 ED 7B 0B 78 94 D5 B5 E8 mple.exe.{.x....
00000030 9E C9 4C 32 24 13 32 62 A0 BC AC 03 12 3D 15 32 ..L2$.2b.....=.2
00000040 06 02 16 03 D1 09 61 22 54 02 43 26 24 BC 04 26 ......a"T.C&$..&
00000050 99 3F CC 0C F3 EA CC FF 27 C4 4A 9D 34 86 42 A7 .?......'.J.4.B.
```

Identifying some common file formats

```
00000000 50 4B 03 04 0A 00 00 00 00 00 25 A5 33 30 8A 94 PK........%.30..
00000010 80 2F 00 3E 00 00 00 3E 00 00 0A 00 00 00 73 61 ./.>...>......sa
00000020 6D 70 6C 65 2E 65 78 65 4D 5A 90 00 03 00 00 00 mple.exeMZ......
00000030 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 ................
00000040 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 @...............
00000050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

Identifying some common file formats

```
00000000 50 4B 03 04 14 00 01 00 00 00 25 A5 33 30 8A 94 PK........%.30..
00000010 80 2F 0C 3E 00 00 00 3E 00 00 0A 00 00 00 73 61 ./.>...>......sa
00000020 6D 70 6C 65 2E 65 78 65 86 72 C6 BD 88 96 EC AA mple.exe.r......
00000030 D3 82 C3 18 85 91 4C C2 A1 0D 61 7C DF 20 2B E9 ......L...a|. +.
00000040 1D 13 1F B4 B1 84 AE 6E F9 49 41 48 E1 07 19 63 .......n.IAH...c
00000050 A8 8C 43 25 82 53 0F 90 FA 07 50 86 C0 6B 79 A4 ..C%.S....P..ky.
```

Identifying some common file formats

```
00000000 52 61 72 21 1A 07 00 CF 90 73 00 00 0D 00 00 00 Rar!.....s......
00000010 00 00 00 00 36 2D 74 20 80 2A 00 00 3E 00 00 00 ....6-t .*..>...
00000020 3E 00 00 02 8A 94 80 2F 25 A5 33 30 14 30 0A 00 >....../%.30.0..
00000030 20 00 00 00 73 61 6D 70 6C 65 2E 65 78 65 4D 5A  ...sample.exeMZ
00000040 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 ................
00000050 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 ......@.........
```

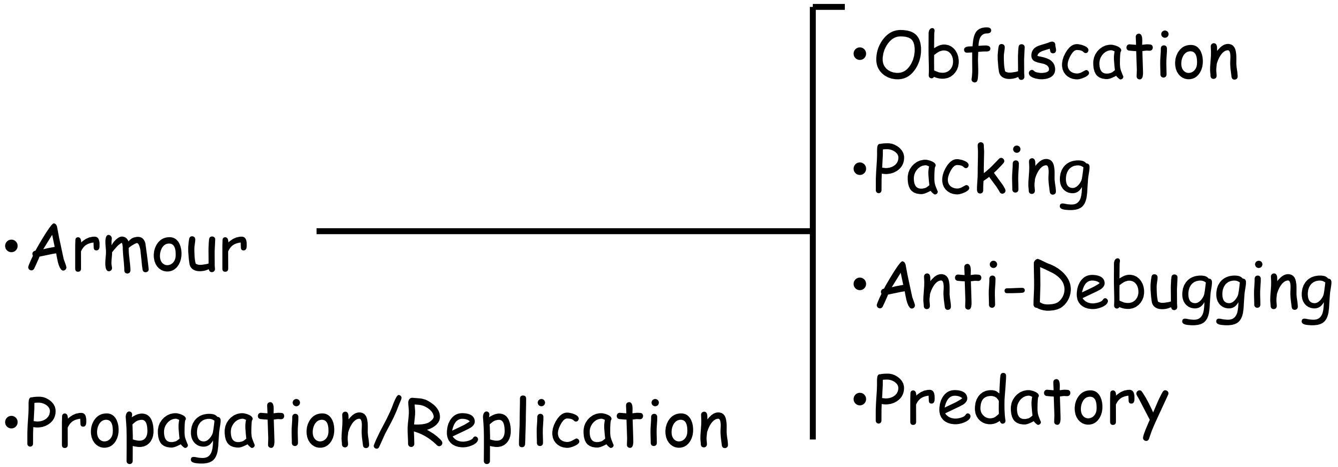
Identifying some common file formats

```
00000000 52 61 72 21 1A 07 00 CE 99 73 80 00 0D 00 00 00 Rar!.....s......
00000010 00 00 00 00 18 D5 17 4F 00 FB 97 C1 70 DC 6E C8 .......O....p.n.
00000020 04 97 55 27 00 58 A1 6D 5C B0 AA 6F 46 1A 95 E8 ..U'.X.m\..oF...
00000030 72 83 91 0F 10 1D D0 77 CF 4B D9 96 B8 28 BB 09 r......w.K...(..
00000040 C3 6B 06 4D 77 3E 67 ED F4 40 F8 5C 20 98 55 D2 .k.Mw>g..@.\ .U.
00000050 69 AE 6F 46 B6 9D 1C 3C 0E 91 69 EF 9E BA 64 EE i.oF...<..i...d.
```

Identifying some common file formats

```
00000000 D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00 ................
00000010 00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00 ........>.......
00000020 06 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 ................
00000030 21 00 00 00 00 00 00 00 00 10 00 00 23 00 00 00 !...........#...
00000040 01 00 00 00 FE FF FF FF 00 00 00 00 20 00 00 00 ............ ...
00000050 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ................
```

Physiology of malware



- Armour
  - Obfuscation
  - Packing
  - Anti-Debugging
  - Predatory
- Propagation/Replication
- Persistance
- Payload/Functionality

Physiology of malware

- Armour
- Propagation/Replication
  - By copy
  - By Email
  - By Exploit
  - By Network
  - By Host infection
- Persistance
- Payload/Functionality

Physiology of malware

- Armour
- Propagation/Replication
- Persistance
  - Autostart folders
  - Registry Run keys
  - Browser Help Objects
  - Creating Service
- Payload/Functionality

Physiology of malware

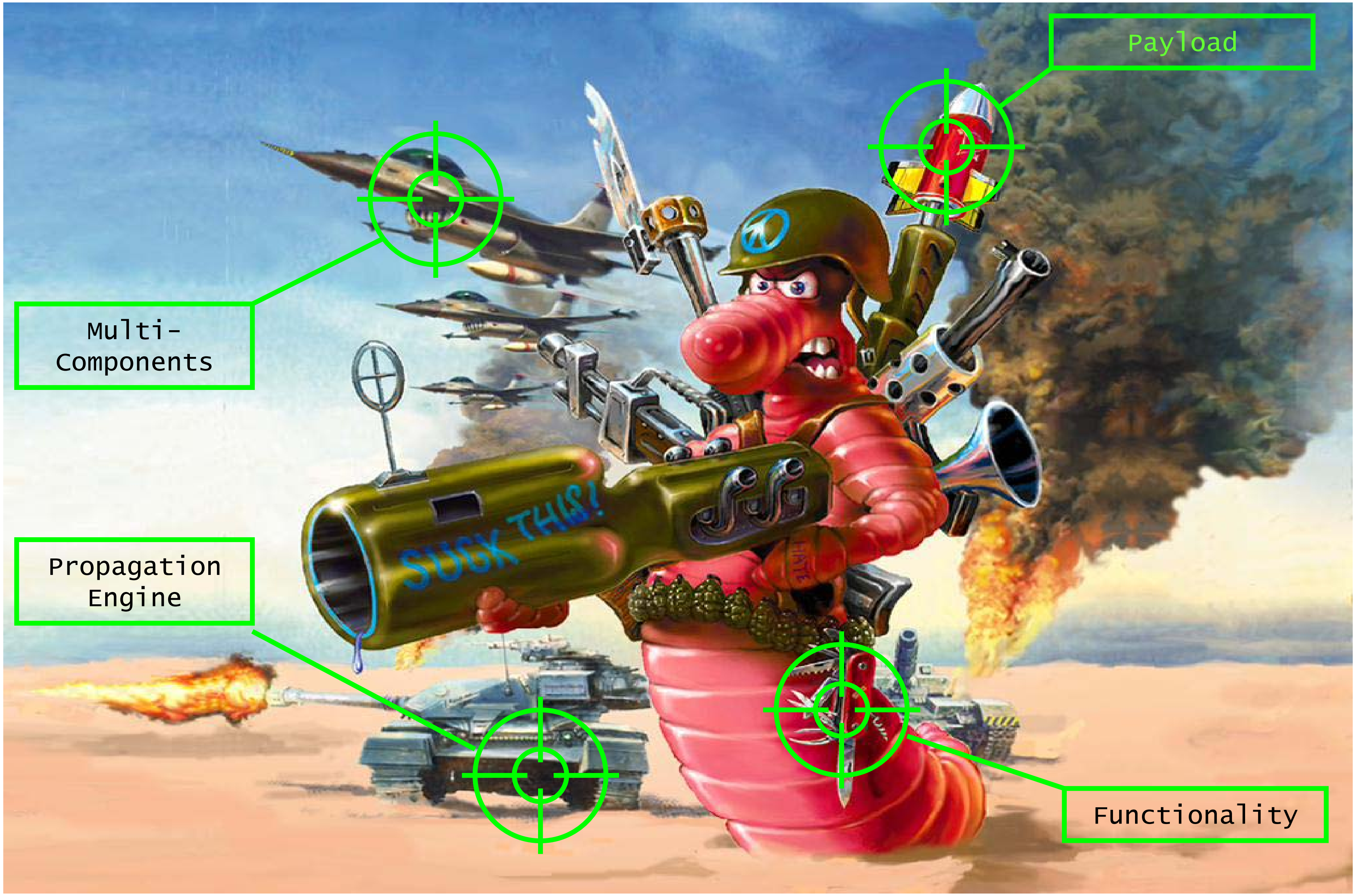
- Armour
- Propagation/Replication
- Persistance
- Payload/Functionality
    - Harmless
    - Spybot
    - Anon. Proxy
    - Data theft or destruction

Trojans

Trojans

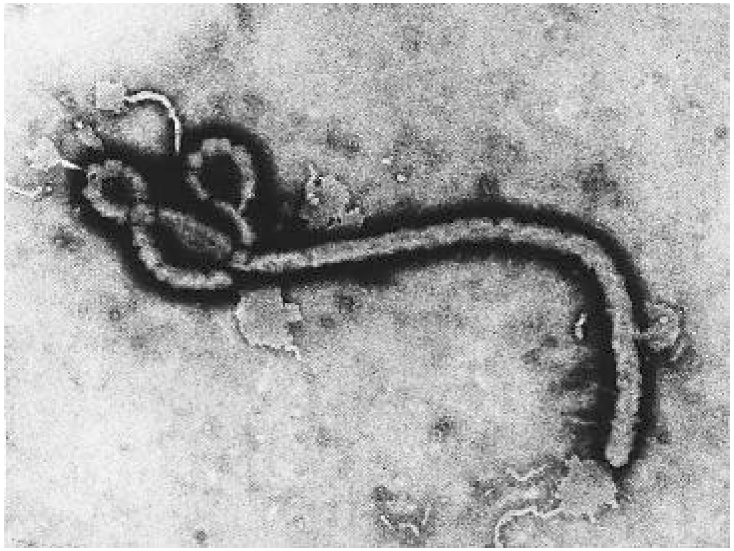
- Appear to be something other than claimed
- Dont replicate
- Size depends on nature of payload
- Typically written in HLL

Worms


Payload
Multi-
Components
Propagation
Engine
Functionality
SUCK THIS!

Viruses (Virii)

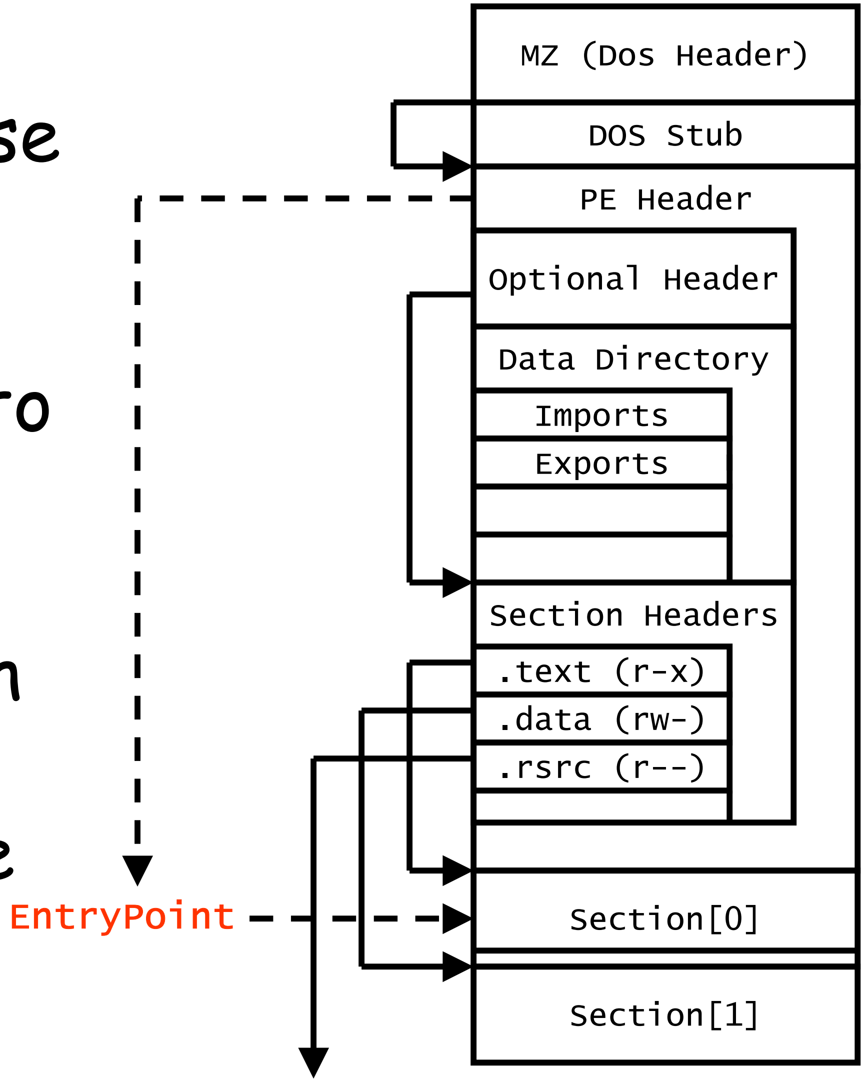
- Replicate by parasitic means (infect files/MBR)
- Intimate knowledge of system data-structures
- Generally written in ASM and are thus small in size



- Majority of authors tend to be skilled individuals and only produce never-released proof-of-concept. Ofcourse there are always going to be bad apples...

Basics of Microsoft PE file

- Unpackers and Viral code make use of intimate knowledge of the PE spec. in order to accomplish their goal. An Analyst being familiar with PE can rapidly identify such code and determine its nature



Toolz of the Trade

- Datarescues Interactive DisAssembler
- SoftIce (debugger)
- Netmon (packet sniffer)
- Tcpmon (sysinternals tcp monitor)
- Regmon (sysinternals registry monitor)
- Filemon (sysinternals file monitor)
- HexWorkshop
- LordPE and/or other PE toolz

Conducting the Analysis

- Lab Environment (inmates running the Assylum)
- Methodical Madness (chase what glitters brightest)
- Keen observation
- Magic numbers arent magic
- Once bitten, twice shy
- Trail of crumbs always leads to a Cookie Monster

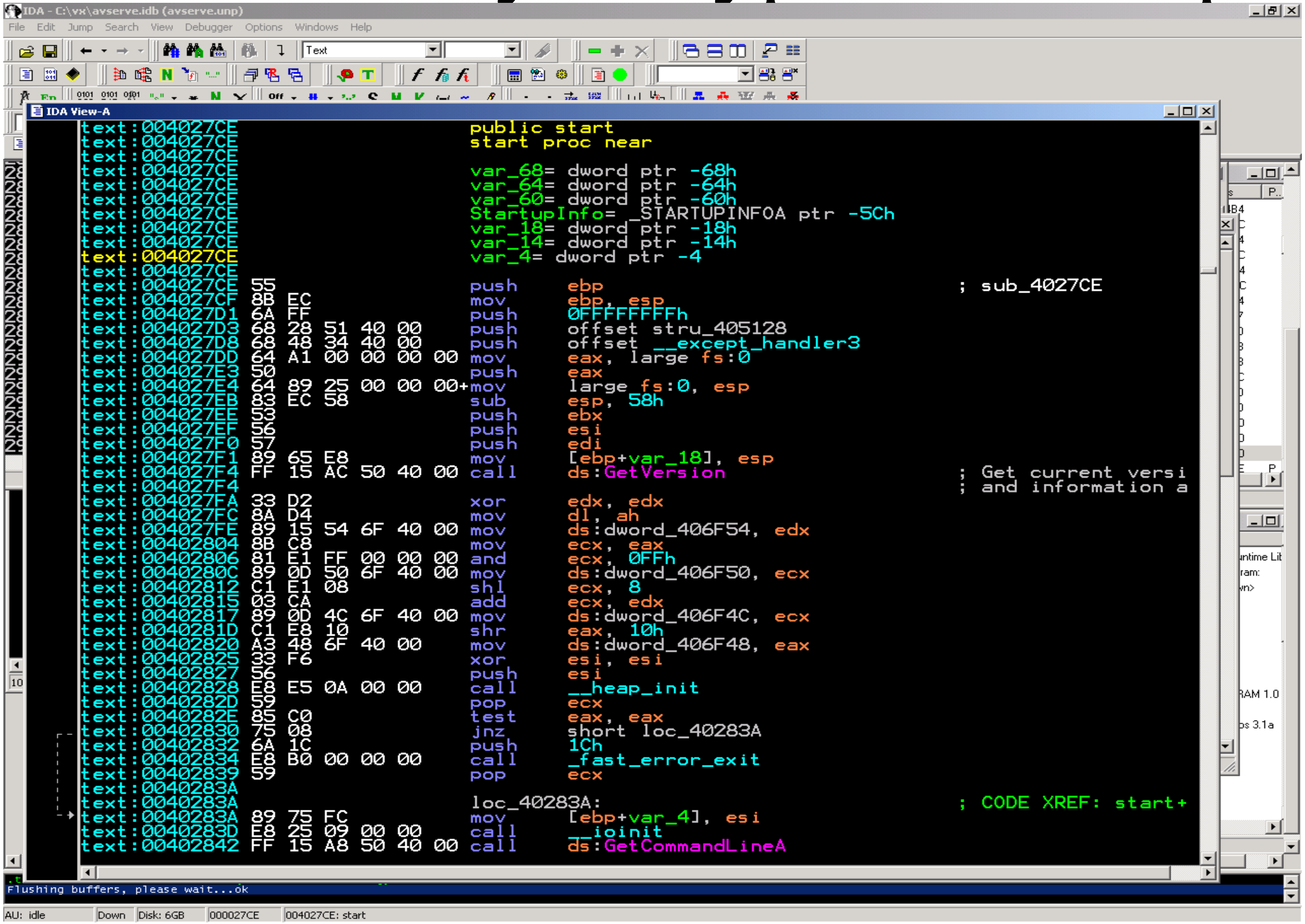
Static (Dead-Listing) Analysis

- Life begins at the EntryPoint
- Functionality flows from Imports
- Services rendered via Exports
- One mans trash is anothers treasure (where have those strings gone?)

Behavioural Analysis

- Involves executing the sample on an isolated network and observing its interaction
- When performed in parallel with static analysis can be used to verify coded behaviour and gain any created data not easily divulged through dead-listing
- Under duress of a debugger, the sample may be stopped at specific locations to examine particular system and sample state(s)

Disassembly of 'typical' startup


IDA - C:\vx\avserve.idb (avserve.unp)
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A

```
text:004027CE                   public start
text:004027CE                   start proc near
text:004027CE
text:004027CE                   var_68= dword ptr -68h
text:004027CE                   var_64= dword ptr -64h
text:004027CE                   var_60= dword ptr -60h
text:004027CE                   StartupInfo= _STARTUPINFOA ptr -5Ch
text:004027CE                   var_18= dword ptr -18h
text:004027CE                   var_14= dword ptr -14h
text:004027CE                   var_4= dword ptr -4
text:004027CE
text:004027CE 55                push    ebp                              ; sub_4027CE
text:004027CF 8B EC             mov     ebp, esp
text:004027D1 6A FF             push    0FFFFFFFFh
text:004027D3 68 28 51 40 00    push    offset stru_405128
text:004027D8 68 48 34 40 00    push    offset __except_handler3
text:004027DD 64 A1 00 00 00 00 mov     eax, large fs:0
text:004027E3 50                push    eax
text:004027E4 64 89 25 00 00 00+mov     large fs:0, esp
text:004027EB 83 EC 58          sub     esp, 58h
text:004027EE 53                push    ebx
text:004027EF 56                push    esi
text:004027F0 57                push    edi
text:004027F1 89 65 E8          mov     [ebp+var_18], esp
text:004027F4 FF 15 AC 50 40 00 call    ds:GetVersion                    ; Get current versi
text:004027F4                                                            ; and information a
text:004027FA 33 D2             xor     edx, edx
text:004027FC 8A D4             mov     dl, ah
text:004027FE 89 15 54 6F 40 00 mov     ds:dword_406F54, edx
text:00402804 8B C8             mov     ecx, eax
text:00402806 81 E1 FF 00 00 00 and     ecx, 0FFh
text:0040280C 89 0D 50 6F 40 00 mov     ds:dword_406F50, ecx
text:00402812 C1 E1 08          shl     ecx, 8
text:00402815 03 CA             add     ecx, edx
text:00402817 89 0D 4C 6F 40 00 mov     ds:dword_406F4C, ecx
text:0040281D C1 E8 10          shr     eax, 10h
text:00402820 A3 48 6F 40 00    mov     ds:dword_406F48, eax
text:00402825 33 F6             xor     esi, esi
text:00402827 56                push    esi
text:00402828 E8 E5 0A 00 00    call    __heap_init
text:0040282D 59                pop     ecx
text:0040282E 85 C0             test    eax, eax
text:00402830 75 08             jnz     short loc_40283A
text:00402832 6A 1C             push    1Ch
text:00402834 E8 B0 00 00 00    call    _fast_error_exit
text:00402839 59                pop     ecx
text:0040283A
text:0040283A                   loc_40283A:                              ; CODE XREF: start+
text:0040283A 89 75 FC          mov     [ebp+var_4], esi
text:0040283D E8 25 09 00 00    call    __ioinit
text:00402842 FF 15 A8 50 40 00 call    ds:GetCommandLineA
```

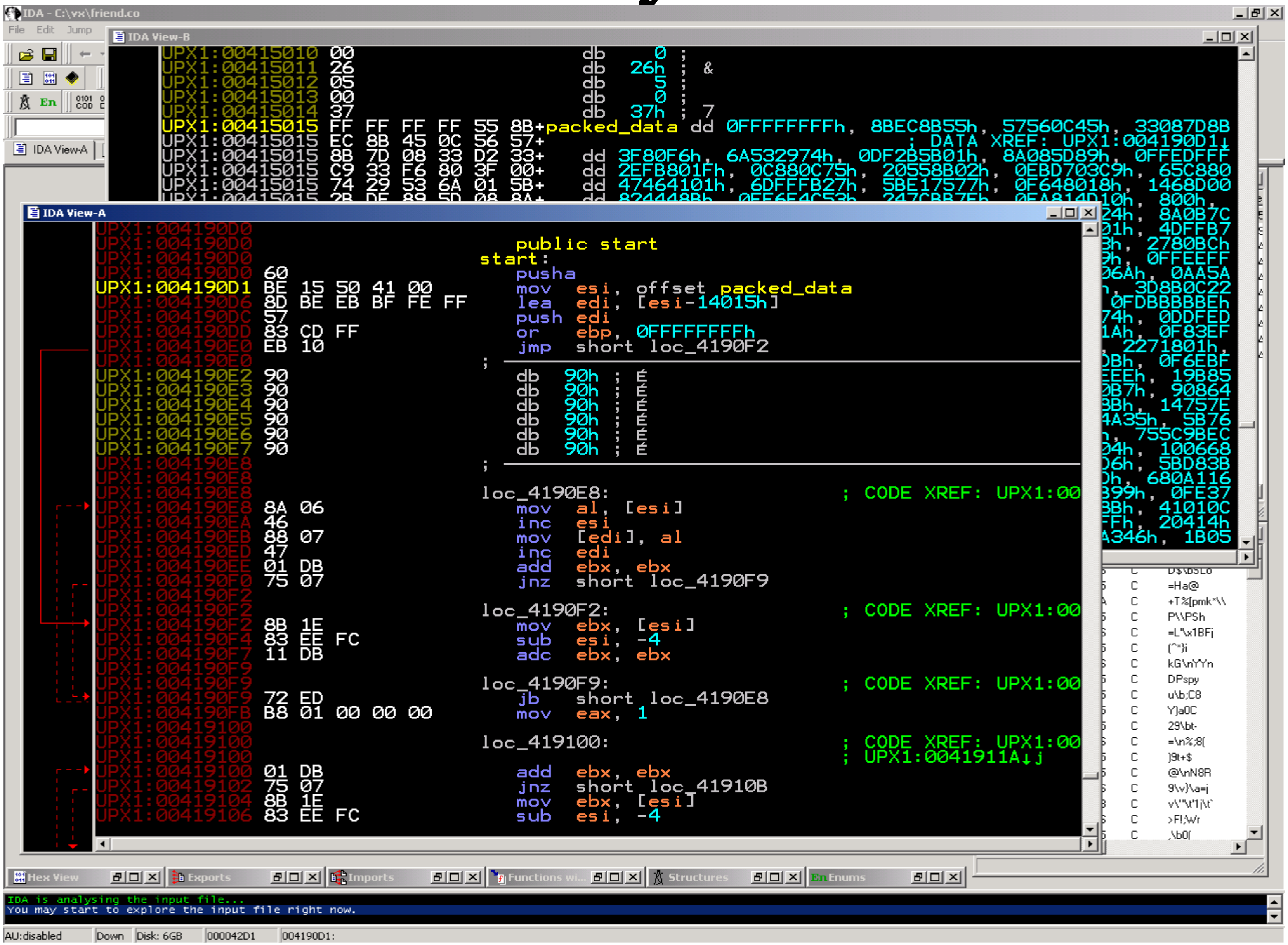
```
Flushing buffers, please wait...ok
```

```
AU: idle    Down    Disk: 6GB    000027CE    004027CE: start
```

Other wonders to be found at EP

- Position Independent Code {Virii, Libs}
- Unpacking code {UPX, FSG, ASPack, etc}
- Decryptors {simple XOR, complex}
- Obfuscation {Morphine}

Have I seen you before ?



```
UPX1:00415010 00                          db    0 ;
UPX1:00415011 26                          db  26h ; &
UPX1:00415012 05                          db    5 ;
UPX1:00415013 00                          db    0 ;
UPX1:00415014 37                          db  37h ; 7
UPX1:00415015 FF FF FF FF 55 8B+packed_data dd 0FFFFFFFFh, 8BEC8B55h, 57560C45h, 33087D8B
UPX1:00415015 EC 8B 45 0C 56 57+                        ; DATA XREF: UPX1:004190D1↓
UPX1:00415015 8B 7D 08 33 D2 33+          dd 3F80F6h, 6A532974h, 0DF2B5B01h, 8A085D89h, 0FFEDFFF
UPX1:00415015 C9 33 F6 80 3F 00+          dd 2EFB801Fh, 0C880C75h, 20558B02h, 0EBD703C9h, 65C880
UPX1:00415015 74 29 53 6A 01 5B+          dd 47464101h, 6DFFFB27h, 5BE17577h, 0F648018h, 1468D00
```

```
UPX1:004190D0
UPX1:004190D0                             public start
UPX1:004190D0                     start:
UPX1:004190D0 60                          pusha
UPX1:004190D1 BE 15 50 41 00              mov     esi, offset packed_data
UPX1:004190D6 8D BE EB BF FE FF           lea     edi, [esi-14015h]
UPX1:004190DC 57                          push    edi
UPX1:004190DD 83 CD FF                    or      ebp, 0FFFFFFFFh
UPX1:004190E0 EB 10                       jmp     short loc_4190F2
UPX1:004190E0                     ; ---------------------------------------------------------
UPX1:004190E2 90                          db  90h ; É
UPX1:004190E3 90                          db  90h ; É
UPX1:004190E4 90                          db  90h ; É
UPX1:004190E5 90                          db  90h ; É
UPX1:004190E6 90                          db  90h ; É
UPX1:004190E7 90                          db  90h ; É
UPX1:004190E8                     ; ---------------------------------------------------------
UPX1:004190E8
UPX1:004190E8                     loc_4190E8:                 ; CODE XREF: UPX1:00
UPX1:004190E8 8A 06                       mov     al, [esi]
UPX1:004190EA 46                          inc     esi
UPX1:004190EB 88 07                       mov     [edi], al
UPX1:004190ED 47                          inc     edi
UPX1:004190EE 01 DB                       add     ebx, ebx
UPX1:004190F0 75 07                       jnz     short loc_4190F9
UPX1:004190F2
UPX1:004190F2                     loc_4190F2:                 ; CODE XREF: UPX1:00
UPX1:004190F2 8B 1E                       mov     ebx, [esi]
UPX1:004190F4 83 EE FC                    sub     esi, -4
UPX1:004190F7 11 DB                       adc     ebx, ebx
UPX1:004190F9
UPX1:004190F9                     loc_4190F9:                 ; CODE XREF: UPX1:00
UPX1:004190F9 72 ED                       jb      short loc_4190E8
UPX1:004190FB B8 01 00 00 00              mov     eax, 1
UPX1:00419100
UPX1:00419100                     loc_419100:                 ; CODE XREF: UPX1:00
UPX1:00419100                                                 ; UPX1:0041911A↓j
UPX1:00419100 01 DB                       add     ebx, ebx
UPX1:00419102 75 07                       jnz     short loc_41910B
UPX1:00419104 8B 1E                       mov     ebx, [esi]
UPX1:00419106 83 EE FC                    sub     esi, -4
```

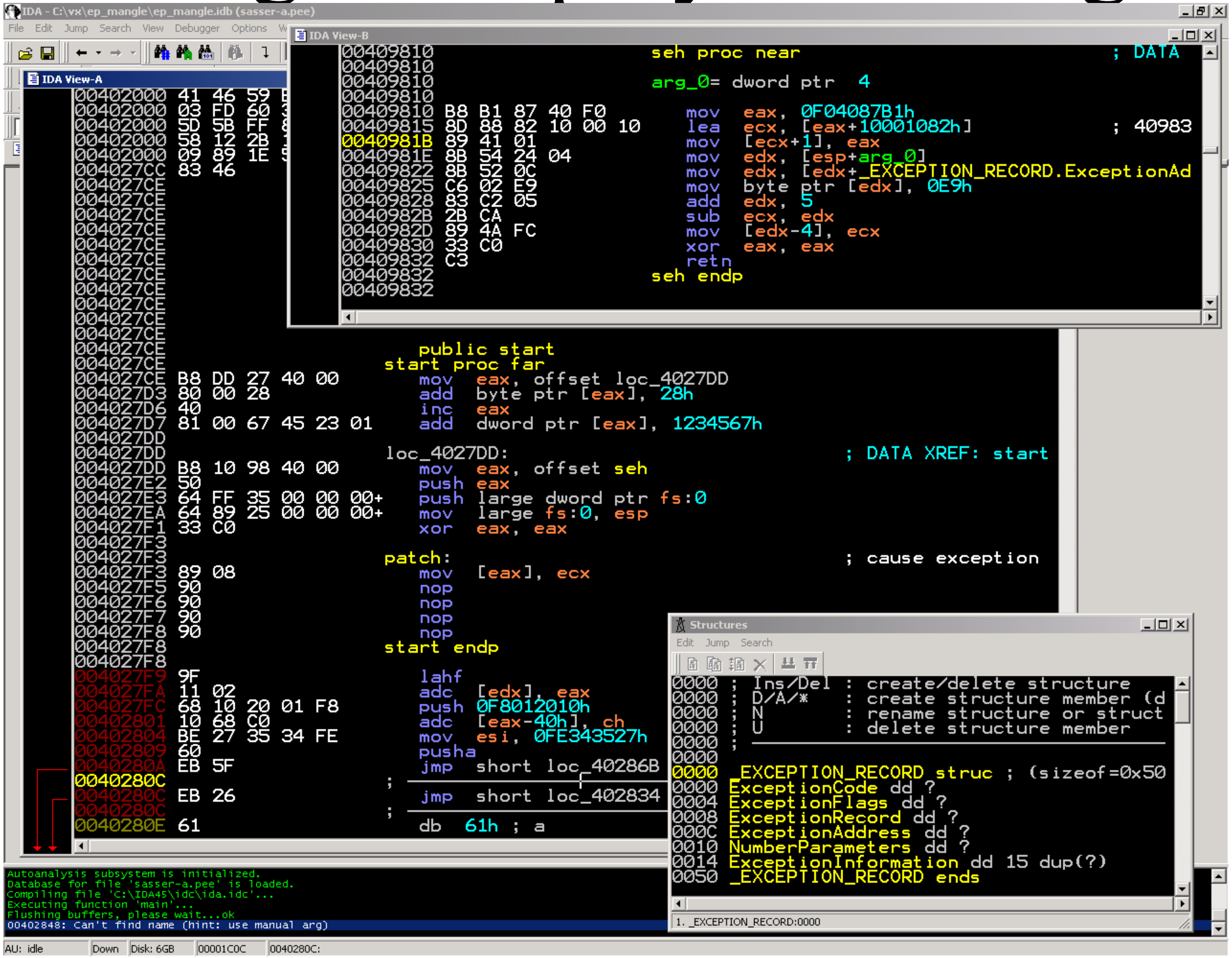
```
0FFEDFFF
65C880
1468D00
10h, 800h,
24h, 8A0B7C
01h, 4DFFB7
3h, 2780BCh
9h, 0FFEEFF
06Ah, 0AA5A
h, 3D8B0C22
0FDBBBBBEh
74h, 0DDFED
1Ah, 0F83EF
, 2271801h,
0Bh, 0F6EBF
EEEh, 19B85
0B7h, 90864
3Bh, 14757E
4A35h, 5B76
h, 755C9BEC
04h, 100668
06h, 5BD83B
0h, 680A116
399h, 0FE37
3Bh, 41010C
FFh, 20414h
A346h, 1B05
```

```
C    =Ha@
C    +T%[pmk*\\
C    P\\PSh
C    =L"\x1BFj
C    (^*}i
C    kG\nYYn
C    DPspy
C    u\b;C8
C    Y)a0C
C    29\bt-
C    =\n%;8(
C    )9t+$
C    @\nN8R
C    9\v}\a=j
C    v\"\t'1j\t`
C    >F!;Wr
C    ,\b0(
```

```
IDA is analysing the input file...
You may start to explore the input file right now.
```

AU:disabled | Down | Disk: 6GB | 000042D1 | 004190D1:

Hiding startup by SEH magic


IDA - C:\vx\ep_mangle\ep_mangle.idb (sasser-a.pee)
File Edit Jump Search View Debugger Options W
IDA View-B
IDA View-A
Structures
Edit Jump Search
AU: idle
Down
Disk: 6GB
00001C0C
0040280C:

```
00409810                    seh proc near                          ; DATA
00409810
00409810                    arg_0= dword ptr  4
00409810
00409810 B8 B1 87 40 F0        mov   eax, 0F04087B1h
00409815 8D 88 82 10 00 10     lea   ecx, [eax+10001082h]          ; 40983
0040981B 89 41 01              mov   [ecx+1], eax
0040981E 8B 54 24 04           mov   edx, [esp+arg_0]
00409822 8B 52 0C              mov   edx, [edx+_EXCEPTION_RECORD.ExceptionAd
00409825 C6 02 E9              mov   byte ptr [edx], 0E9h
00409828 83 C2 05              add   edx, 5
0040982B 2B CA                 sub   ecx, edx
0040982D 89 4A FC              mov   [edx-4], ecx
00409830 33 C0                 xor   eax, eax
00409832 C3                    retn
00409832                    seh endp
00409832
```

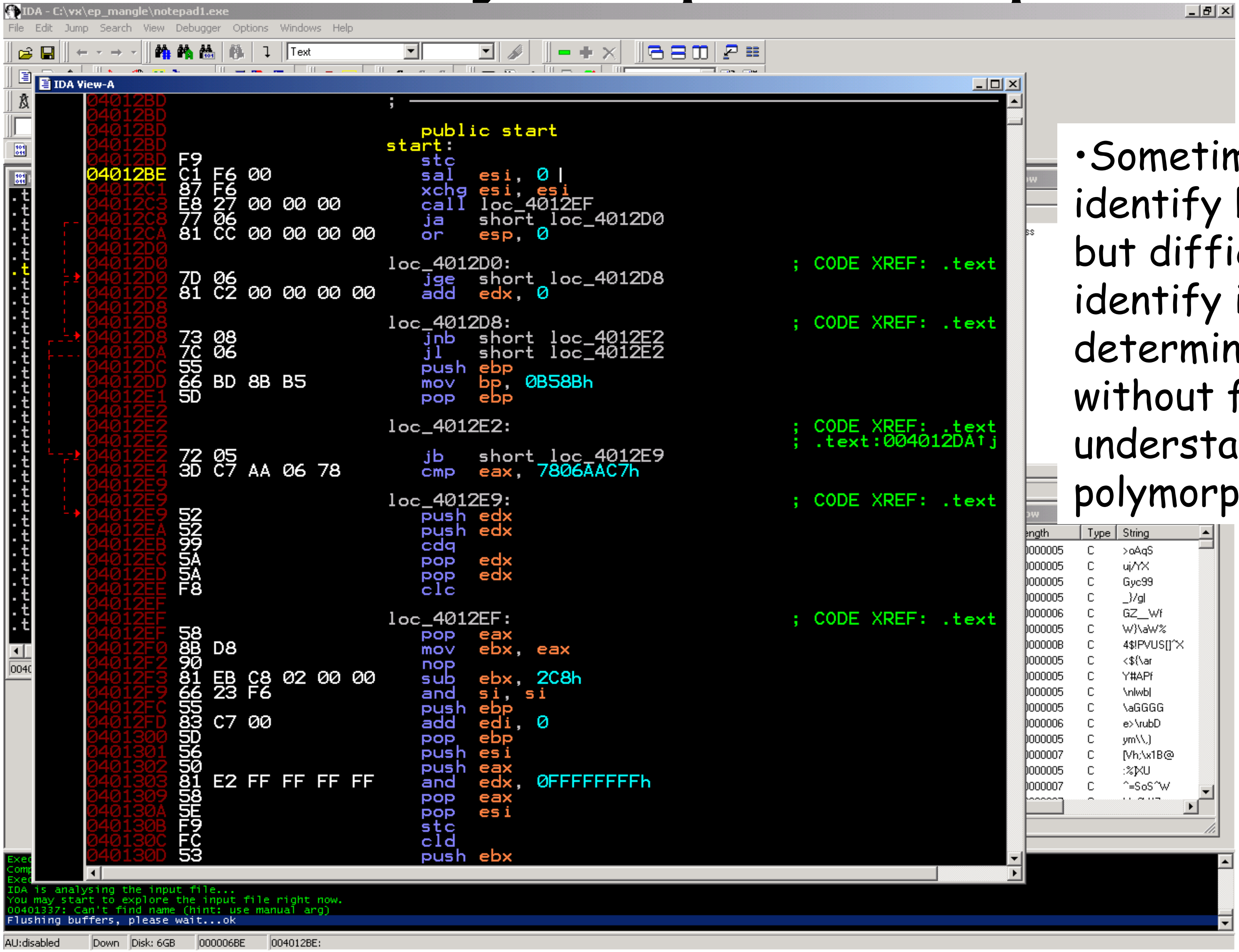
```
00402000 41 46 59 E
00402000 03 FD 60 3
00402000 5D 5B FF 8
00402000 58 12 2B 1
00402000 09 89 1E 5
004027CC 83 46
004027CE
004027CE
004027CE
004027CE
004027CE
004027CE
004027CE
004027CE
004027CE
004027CE
004027CE
004027CE
004027CE
004027CE                    public start
004027CE                    start proc far
004027CE B8 DD 27 40 00        mov   eax, offset loc_4027DD
004027D3 80 00 28              add   byte ptr [eax], 28h
004027D6 40                    inc   eax
004027D7 81 00 67 45 23 01     add   dword ptr [eax], 1234567h
004027DD
004027DD                    loc_4027DD:                          ; DATA XREF: start
004027DD B8 10 98 40 00        mov   eax, offset seh
004027E2 50                    push  eax
004027E3 64 FF 35 00 00 00+    push  large dword ptr fs:0
004027EA 64 89 25 00 00 00+    mov   large fs:0, esp
004027F1 33 C0                 xor   eax, eax
004027F3
004027F3                    patch:                               ; cause exception
004027F3 89 08                 mov   [eax], ecx
004027F5 90                    nop
004027F6 90                    nop
004027F7 90                    nop
004027F8 90                    nop
004027F8                    start endp
004027F8
004027F9 9F                    lahf
004027FA 11 02                 adc   [edx], eax
004027FC 68 10 20 01 F8        push  0F8012010h
00402801 10 68 C0              adc   [eax-40h], ch
00402804 BE 27 35 34 FE        mov   esi, 0FE343527h
00402809 60                    pusha
0040280A EB 5F                 jmp   short loc_40286B
0040280C                    ; ─────────────────────────
0040280C EB 26                 jmp   short loc_402834
0040280C                    ; ─────────────────────────
0040280E 61                    db  61h ; a
```

```
0000 ; Ins/Del   : create/delete structure
0000 ; D/A/*     : create structure member (d
0000 ; N         : rename structure or struct
0000 ; U         : delete structure member
0000 ;
0000
0000 _EXCEPTION_RECORD struc ; (sizeof=0x50
0000 ExceptionCode dd ?
0004 ExceptionFlags dd ?
0008 ExceptionRecord dd ?
000C ExceptionAddress dd ?
0010 NumberParameters dd ?
0014 ExceptionInformation dd 15 dup(?)
0050 _EXCEPTION_RECORD ends
```

1. _EXCEPTION_RECORD:0000

```
Autoanalysis subsystem is initialized.
Database for file 'sasser-a.pee' is loaded.
Compiling file 'C:\IDA45\idc\ida.idc'...
Executing function 'main'...
Flushing buffers, please wait...ok
00402848: Can't find name (hint: use manual arg)
```

Polymorphic Tarpit



IDA - C:\vx\ep_mangle\notepad1.exe
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A

```
04012BD                         ; ---------------------------------------------
04012BD
04012BD                            public start
04012BD                         start:
04012BD F9                         stc
04012BE C1 F6 00                   sal  esi, 0
04012C1 87 F6                      xchg esi, esi
04012C3 E8 27 00 00 00             call loc_4012EF
04012C8 77 06                      ja   short loc_4012D0
04012CA 81 CC 00 00 00 00          or   esp, 0
04012D0
04012D0                         loc_4012D0:                          ; CODE XREF: .text
04012D0 7D 06                      jge  short loc_4012D8
04012D2 81 C2 00 00 00 00          add  edx, 0
04012D8
04012D8                         loc_4012D8:                          ; CODE XREF: .text
04012D8 73 08                      jnb  short loc_4012E2
04012DA 7C 06                      jl   short loc_4012E2
04012DC 55                         push ebp
04012DD 66 BD 8B B5                mov  bp, 0B58Bh
04012E1 5D                         pop  ebp
04012E2
04012E2                         loc_4012E2:                          ; CODE XREF: .text
04012E2                                                              ; .text:004012DA↑j
04012E2 72 05                      jb   short loc_4012E9
04012E4 3D C7 AA 06 78             cmp  eax, 7806AAC7h
04012E9
04012E9                         loc_4012E9:                          ; CODE XREF: .text
04012E9 52                         push edx
04012EA 52                         push edx
04012EB 99                         cdq
04012EC 5A                         pop  edx
04012ED 5A                         pop  edx
04012EE F8                         clc
04012EF
04012EF                         loc_4012EF:                          ; CODE XREF: .text
04012EF 58                         pop  eax
04012F0 8B D8                      mov  ebx, eax
04012F2 90                         nop
04012F3 81 EB C8 02 00 00          sub  ebx, 2C8h
04012F9 66 23 F6                   and  si, si
04012FC 55                         push ebp
04012FD 83 C7 00                   add  edi, 0
0401300 5D                         pop  ebp
0401301 56                         push esi
0401302 50                         push eax
0401303 81 E2 FF FF FF FF          and  edx, 0FFFFFFFFh
0401309 58                         pop  eax
040130A 5E                         pop  esi
040130B F9                         stc
040130C FC                         cld
040130D 53                         push ebx
```

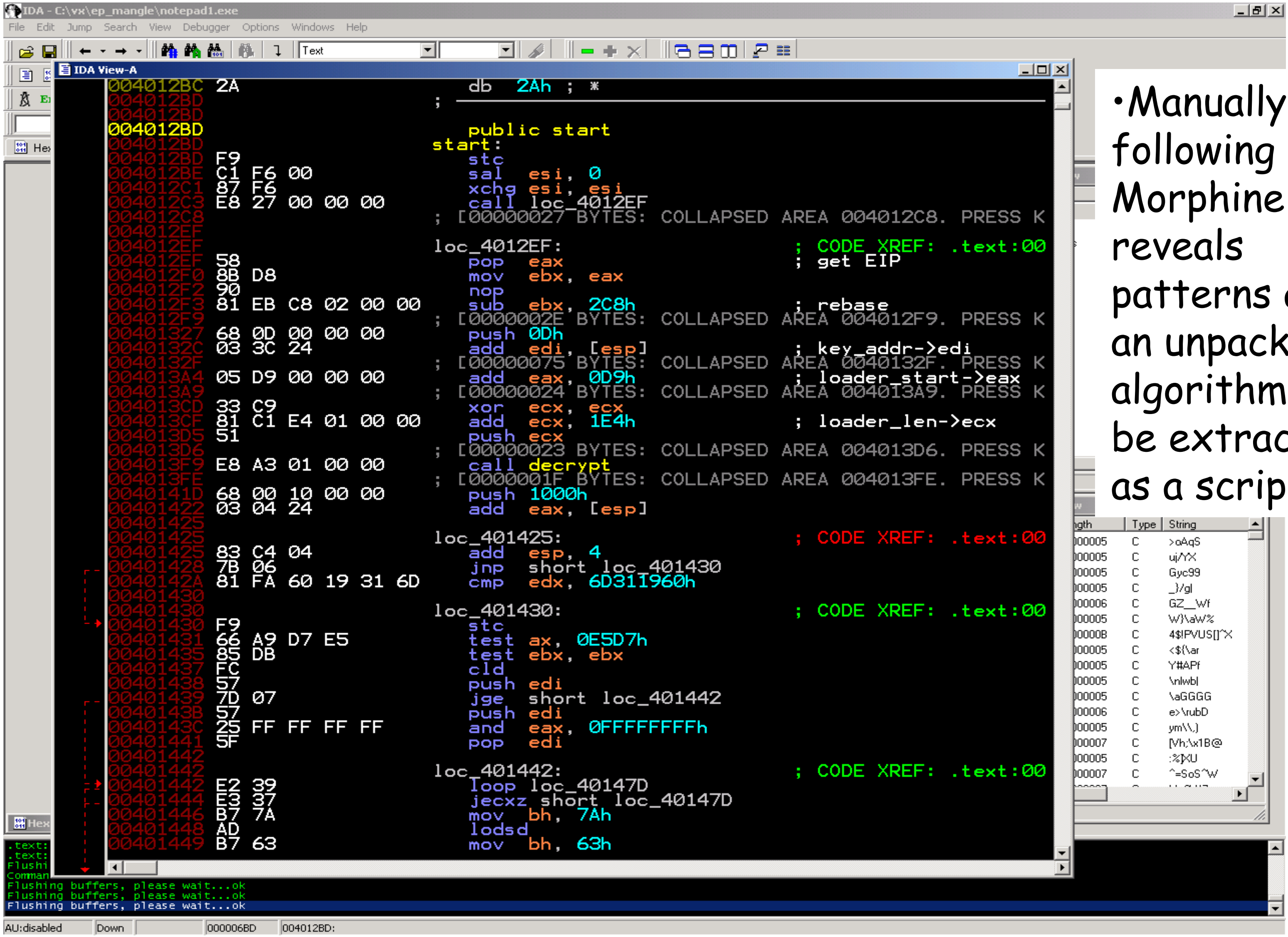
ength	Type	String
0000005	C	>αAqS
0000005	C	uj/YX
0000005	C	Gyc99
0000005	C	_}/gl
0000006	C	GZ__Wf
0000005	C	W}\aW%
000000B	C	4$!PVUS[]^X
0000005	C	<${\ar
0000005	C	Y#APf
0000005	C	\nlwbl
0000005	C	\aGGGG
0000006	C	e>\rubD
0000005	C	ym\\.)
0000007	C	[Vh;\x1B@
0000005	C	:%]XU
0000007	C	^=SoS^W

```
Exec
Comp
Exec
IDA is analysing the input file...
You may start to explore the input file right now.
00401337: Can't find name (hint: use manual arg)
Flushing buffers, please wait...ok
```

AU:disabled | Down | Disk: 6GB | 000006BE | 004012BE:

- Sometimes easy to identify by a human but difficult to identify in a deterministic way without first fully understanding the polymorphic engine.

Unravelling Morphine



```
004012BC 2A                          db   2Ah ; *
004012BD                       ; ─────────────────────────────────────────────
004012BD
004012BD                             public start
004012BD                       start:
004012BD F9                          stc
004012BE C1 F6 00                    sal   esi, 0
004012C1 87 F6                       xchg  esi, esi
004012C3 E8 27 00 00 00              call  loc_4012EF
004012C8                       ; [00000027 BYTES: COLLAPSED AREA 004012C8. PRESS K
004012EF
004012EF                       loc_4012EF:                      ; CODE XREF: .text:00
004012EF 58                          pop   eax                  ; get EIP
004012F0 8B D8                       mov   ebx, eax
004012F2 90                          nop
004012F3 81 EB C8 02 00 00           sub   ebx, 2C8h            ; rebase
004012F9                       ; [0000002E BYTES: COLLAPSED AREA 004012F9. PRESS K
00401327 68 0D 00 00 00              push 0Dh
0040132C 03 3C 24                    add   edi, [esp]           ; key_addr->edi
0040132F                       ; [00000075 BYTES: COLLAPSED AREA 0040132F. PRESS K
004013A4 05 D9 00 00 00              add   eax, 0D9h            ; loader_start->eax
004013A9                       ; [00000024 BYTES: COLLAPSED AREA 004013A9. PRESS K
004013CD 33 C9                       xor   ecx, ecx
004013CF 81 C1 E4 01 00 00           add   ecx, 1E4h            ; loader_len->ecx
004013D5 51                          push ecx
004013D6                       ; [00000023 BYTES: COLLAPSED AREA 004013D6. PRESS K
004013F9 E8 A3 01 00 00              call decrypt
004013FE                       ; [0000001F BYTES: COLLAPSED AREA 004013FE. PRESS K
0040141D 68 00 10 00 00              push 1000h
00401422 03 04 24                    add   eax, [esp]
00401425
00401425                       loc_401425:                      ; CODE XREF: .text:00
00401425 83 C4 04                    add   esp, 4
00401428 7B 06                       jnp   short loc_401430
0040142A 81 FA 60 19 31 6D           cmp   edx, 6D311960h
00401430
00401430                       loc_401430:                      ; CODE XREF: .text:00
00401430 F9                          stc
00401431 66 A9 D7 E5                 test ax, 0E5D7h
00401435 85 DB                       test ebx, ebx
00401437 FC                          cld
00401438 57                          push edi
00401439 7D 07                       jge   short loc_401442
0040143B 57                          push edi
0040143C 25 FF FF FF FF              and   eax, 0FFFFFFFFh
00401441 5F                          pop   edi
00401442
00401442                       loc_401442:                      ; CODE XREF: .text:00
00401442 E2 39                       loop loc_40147D
00401444 E3 37                       jecxz short loc_40147D
00401446 B7 7A                       mov   bh, 7Ah
00401448 AD                          lodsd
00401449 B7 63                       mov   bh, 63h
```

ngth	Type	String
000005	C	>αAqS
000005	C	uj/YX
000005	C	Gyc99
000005	C	_}/gl
000006	C	GZ__Wf
000005	C	W}\aW%
00000B	C	4$!PVUS[]^X
000005	C	<${\ar
000005	C	Y#APf
000005	C	\nlwbl
000005	C	\aGGGG
000006	C	e>\rubD
000005	C	ym\\,)
000007	C	[Vh;\x1B@
000005	C	:%]XU
000007	C	^=SoS^W

```
.text:
.text:
Flushi
Comman
Flushing buffers, please wait...ok
Flushing buffers, please wait...ok
Flushing buffers, please wait...ok
```

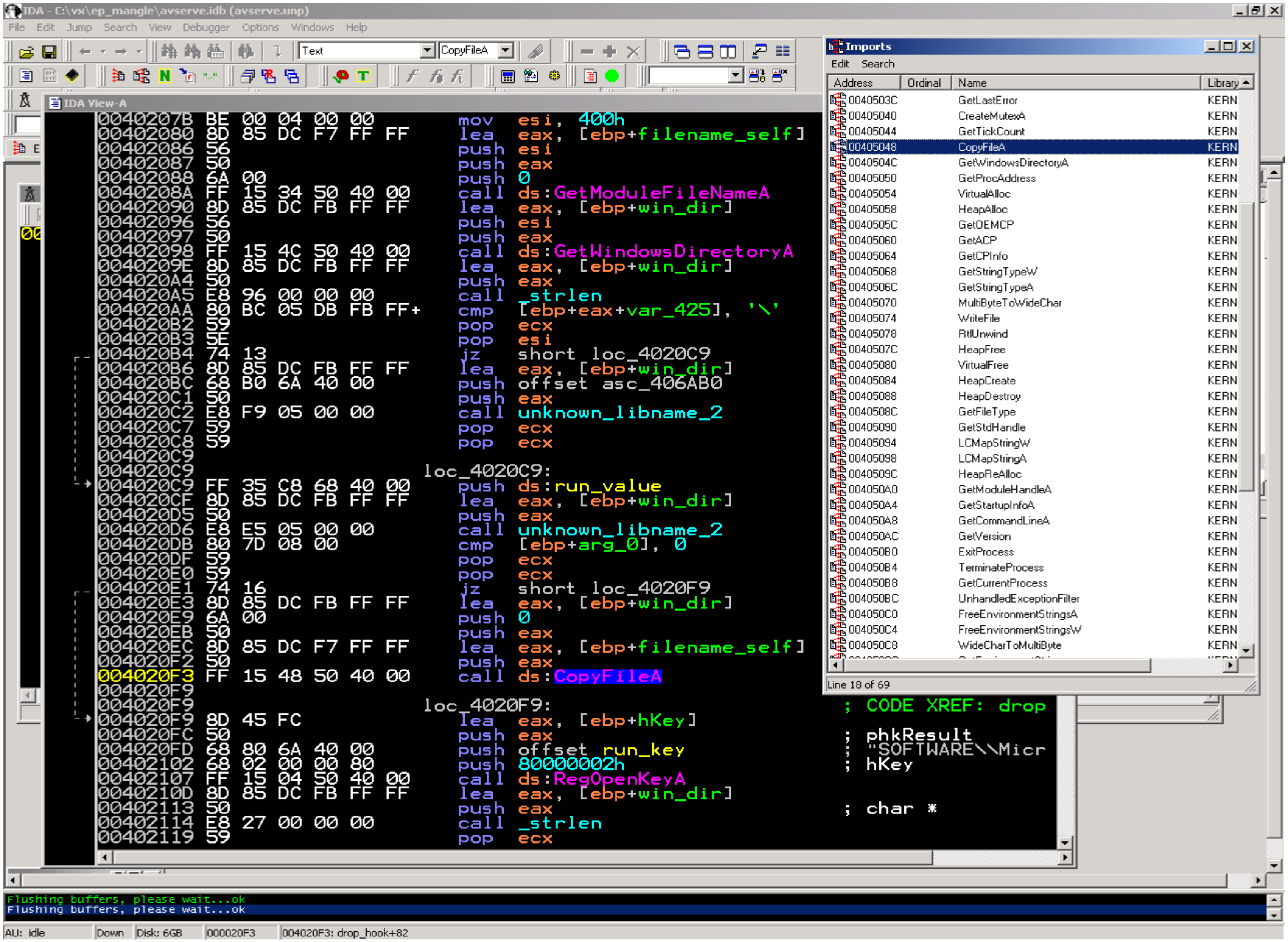
AU:disabled | Down | 000006BD | 004012BD:

- Manually following Morphine code reveals patterns and an unpacking algorithm can be extracted as a script

Imports, sign-posts to functionality

- Examination of the Imports is a good starting point when fishing for malicious code blocks
- In order to satisfy Persistance, most malware will use a handfull of well defined APIs such as CopyFileA, MoveFileA, CreateFileA, RegCreateKey

Import Following - CopyFileA


IDA - C:\vx\ep_mangle\avserve.idb (avserve.unp)
File Edit Jump Search View Debugger Options Windows Help
Text
CopyFileA
IDA View-A
Imports
Edit Search

```
0040207B BE 00 04 00 00          mov   esi, 400h
00402080 8D 85 DC F7 FF FF       lea   eax, [ebp+filename_self]
00402086 56                      push  esi
00402087 50                      push  eax
00402088 6A 00                   push  0
0040208A FF 15 34 50 40 00       call  ds:GetModuleFileNameA
00402090 8D 85 DC FB FF FF       lea   eax, [ebp+win_dir]
00402096 56                      push  esi
00402097 50                      push  eax
00402098 FF 15 4C 50 40 00       call  ds:GetWindowsDirectoryA
0040209E 8D 85 DC FB FF FF       lea   eax, [ebp+win_dir]
004020A4 50                      push  eax
004020A5 E8 96 00 00 00          call  _strlen
004020AA 80 BC 05 DB FB FF+      cmp   [ebp+eax+var_425], '\'
004020B2 59                      pop   ecx
004020B3 5E                      pop   esi
004020B4 74 13                   jz    short loc_4020C9
004020B6 8D 85 DC FB FF FF       lea   eax, [ebp+win_dir]
004020BC 68 B0 6A 40 00          push  offset asc_406AB0
004020C1 50                      push  eax
004020C2 E8 F9 05 00 00          call  unknown_libname_2
004020C7 59                      pop   ecx
004020C8 59                      pop   ecx
004020C9
004020C9                     loc_4020C9:
004020C9 FF 35 C8 68 40 00       push  ds:run_value
004020CF 8D 85 DC FB FF FF       lea   eax, [ebp+win_dir]
004020D5 50                      push  eax
004020D6 E8 E5 05 00 00          call  unknown_libname_2
004020DB 80 7D 08 00             cmp   [ebp+arg_0], 0
004020DF 59                      pop   ecx
004020E0 59                      pop   ecx
004020E1 74 16                   jz    short loc_4020F9
004020E3 8D 85 DC FB FF FF       lea   eax, [ebp+win_dir]
004020E9 6A 00                   push  0
004020EB 50                      push  eax
004020EC 8D 85 DC F7 FF FF       lea   eax, [ebp+filename_self]
004020F2 50                      push  eax
004020F3 FF 15 48 50 40 00       call  ds:CopyFileA
004020F9
004020F9                     loc_4020F9:                          ; CODE XREF: drop
004020F9 8D 45 FC                lea   eax, [ebp+hKey]
004020FC 50                      push  eax                        ; phkResult
004020FD 68 80 6A 40 00          push  offset run_key             ; "SOFTWARE\\Micr
00402102 68 02 00 00 80          push  80000002h                  ; hKey
00402107 FF 15 04 50 40 00       call  ds:RegOpenKeyA
0040210D 8D 85 DC FB FF FF       lea   eax, [ebp+win_dir]
00402113 50                      push  eax                        ; char *
00402114 E8 27 00 00 00          call  _strlen
00402119 59                      pop   ecx
```

Address	Ordinal	Name	Library
0040503C		GetLastError	KERN
00405040		CreateMutexA	KERN
00405044		GetTickCount	KERN
00405048		CopyFileA	KERN
0040504C		GetWindowsDirectoryA	KERN
00405050		GetProcAddress	KERN
00405054		VirtualAlloc	KERN
00405058		HeapAlloc	KERN
0040505C		GetOEMCP	KERN
00405060		GetACP	KERN
00405064		GetCPInfo	KERN
00405068		GetStringTypeW	KERN
0040506C		GetStringTypeA	KERN
00405070		MultiByteToWideChar	KERN
00405074		WriteFile	KERN
00405078		RtlUnwind	KERN
0040507C		HeapFree	KERN
00405080		VirtualFree	KERN
00405084		HeapCreate	KERN
00405088		HeapDestroy	KERN
0040508C		GetFileType	KERN
00405090		GetStdHandle	KERN
00405094		LCMapStringW	KERN
00405098		LCMapStringA	KERN
0040509C		HeapReAlloc	KERN
004050A0		GetModuleHandleA	KERN
004050A4		GetStartupInfoA	KERN
004050A8		GetCommandLineA	KERN
004050AC		GetVersion	KERN
004050B0		ExitProcess	KERN
004050B4		TerminateProcess	KERN
004050B8		GetCurrentProcess	KERN
004050BC		UnhandledExceptionFilter	KERN
004050C0		FreeEnvironmentStringsA	KERN
004050C4		FreeEnvironmentStringsW	KERN
004050C8		WideCharToMultiByte	KERN

Line 18 of 69

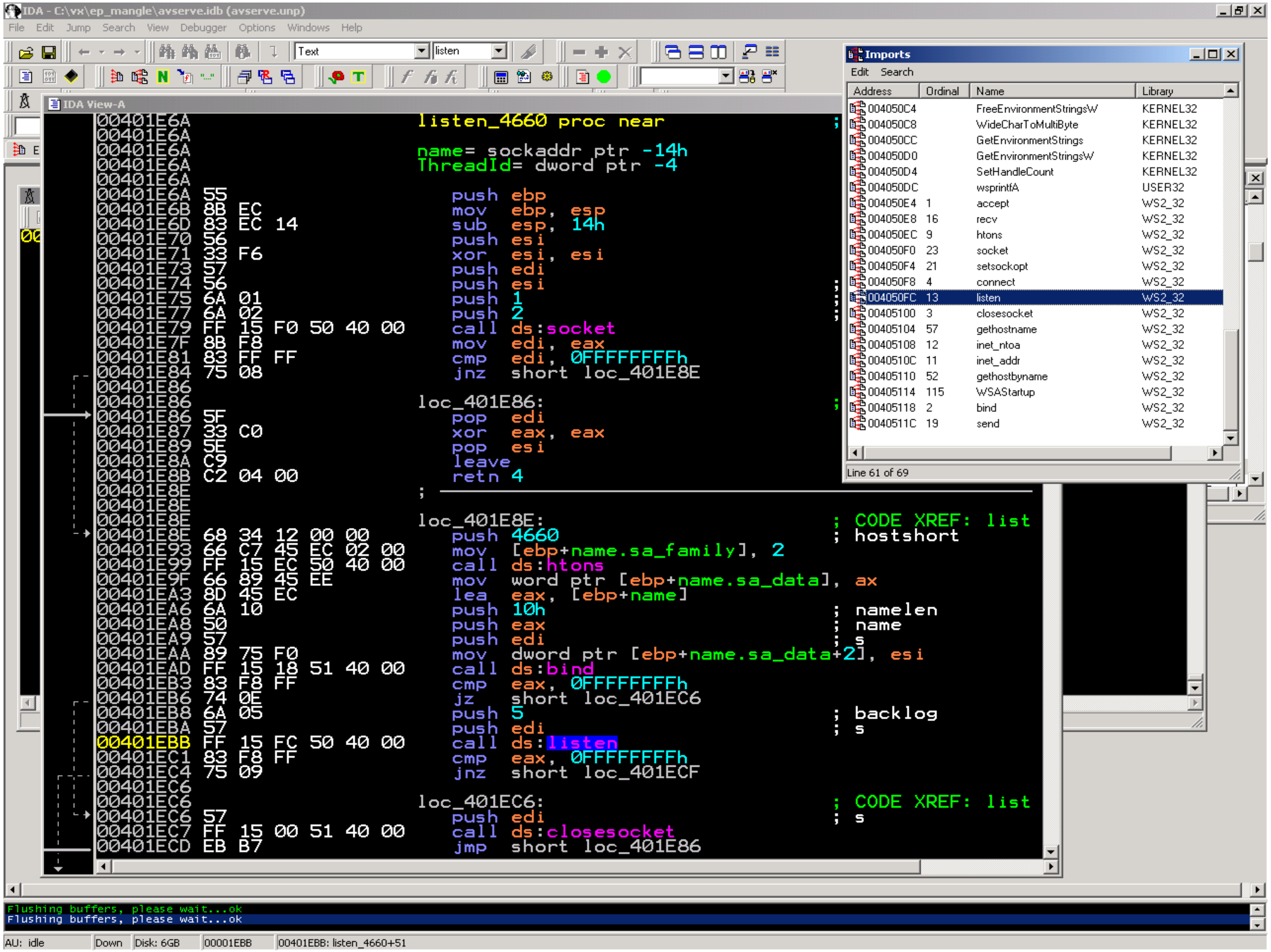
```
Flushing buffers, please wait...ok
Flushing buffers, please wait...ok
```

AU: idle | Down | Disk: 6GB | 000020F3 | 004020F3: drop_hook+82

Imports, sign-posts to functionality

- If the malware includes networking capability its Imports will show this
- Malware of the Viral variety often calls upon MapViewOfFileA during infection
- Malware which spreads by email may contain its own SMTP engine (which can be found by following socket APIs)
- Trojans and backdoor bots often run listen servers awaiting commands

Import Following - listen



IDA - C:\vx\ep_mangle\avserve.idb (avserve.unp)
File Edit Jump Search View Debugger Options Windows Help
Text
listen
IDA View-A

```
00401E6A                    listen_4660 proc near                      ;
00401E6A
00401E6A                    name= sockaddr ptr -14h
00401E6A                    ThreadId= dword ptr -4
00401E6A
00401E6A 55                    push  ebp
00401E6B 8B EC                 mov   ebp, esp
00401E6D 83 EC 14              sub   esp, 14h
00401E70 56                    push  esi
00401E71 33 F6                 xor   esi, esi
00401E73 57                    push  edi
00401E74 56                    push  esi                               ;
00401E75 6A 01                 push  1                                 ;
00401E77 6A 02                 push  2                                 ;
00401E79 FF 15 F0 50 40 00     call  ds:socket
00401E7F 8B F8                 mov   edi, eax
00401E81 83 FF FF              cmp   edi, 0FFFFFFFFh
00401E84 75 08                 jnz   short loc_401E8E
00401E86
00401E86                    loc_401E86:                                ;
00401E86 5F                    pop   edi
00401E87 33 C0                 xor   eax, eax
00401E89 5E                    pop   esi
00401E8A C9                    leave
00401E8B C2 04 00              retn  4
00401E8E                    ;
00401E8E
00401E8E                    loc_401E8E:                                ; CODE XREF: list
00401E8E 68 34 12 00 00        push  4660                              ; hostshort
00401E93 66 C7 45 EC 02 00     mov   [ebp+name.sa_family], 2
00401E99 FF 15 EC 50 40 00     call  ds:htons
00401E9F 66 89 45 EE           mov   word ptr [ebp+name.sa_data], ax
00401EA3 8D 45 EC              lea   eax, [ebp+name]
00401EA6 6A 10                 push  10h                               ; namelen
00401EA8 50                    push  eax                               ; name
00401EA9 57                    push  edi                               ; s
00401EAA 89 75 F0              mov   dword ptr [ebp+name.sa_data+2], esi
00401EAD FF 15 18 51 40 00     call  ds:bind
00401EB3 83 F8 FF              cmp   eax, 0FFFFFFFFh
00401EB6 74 0E                 jz    short loc_401EC6
00401EB8 6A 05                 push  5                                 ; backlog
00401EBA 57                    push  edi                               ; s
00401EBB FF 15 FC 50 40 00     call  ds:listen
00401EC1 83 F8 FF              cmp   eax, 0FFFFFFFFh
00401EC4 75 09                 jnz   short loc_401ECF
00401EC6
00401EC6                    loc_401EC6:                                ; CODE XREF: list
00401EC6 57                    push  edi                               ; s
00401EC7 FF 15 00 51 40 00     call  ds:closesocket
00401ECD EB B7                 jmp   short loc_401E86
```

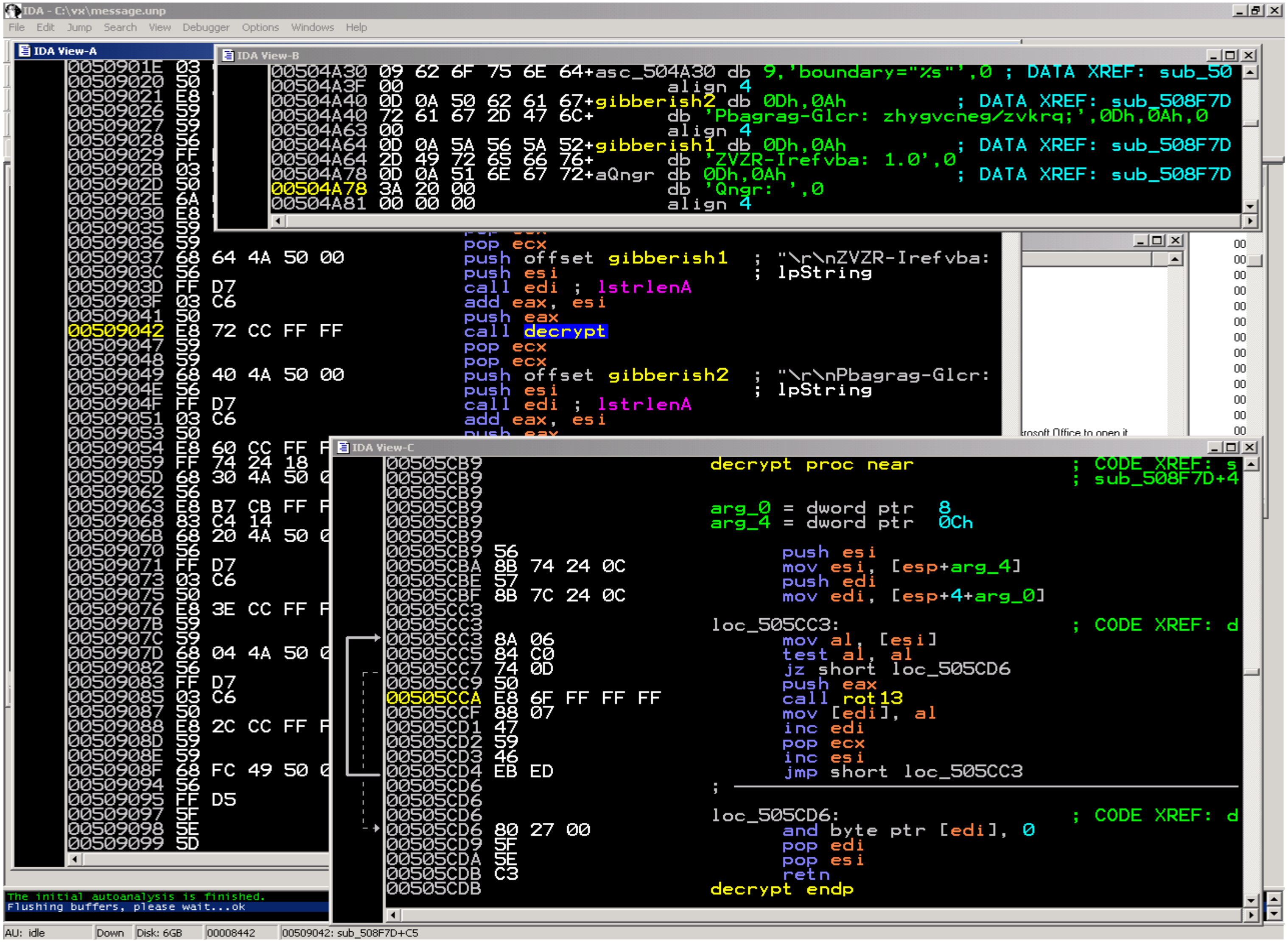
Address	Ordinal	Name	Library
004050C4		FreeEnvironmentStringsW	KERNEL32
004050C8		WideCharToMultiByte	KERNEL32
004050CC		GetEnvironmentStrings	KERNEL32
004050D0		GetEnvironmentStringsW	KERNEL32
004050D4		SetHandleCount	KERNEL32
004050DC		wsprintfA	USER32
004050E4	1	accept	WS2_32
004050E8	16	recv	WS2_32
004050EC	9	htons	WS2_32
004050F0	23	socket	WS2_32
004050F4	21	setsockopt	WS2_32
004050F8	4	connect	WS2_32
004050FC	13	listen	WS2_32
00405100	3	closesocket	WS2_32
00405104	57	gethostname	WS2_32
00405108	12	inet_ntoa	WS2_32
0040510C	11	inet_addr	WS2_32
00405110	52	gethostbyname	WS2_32
00405114	115	WSAStartup	WS2_32
00405118	2	bind	WS2_32
0040511C	19	send	WS2_32

Line 61 of 69

```
Flushing buffers, please wait...ok
Flushing buffers, please wait...ok
```

AU: idle | Down | Disk: 6GB | 00001EBB | 00401EBB: listen_4660+51

Where did I put my Babel fish ?



IDA View-B

```
00504A30 09 62 6F 75 6E 64+asc_504A30 db 9,'boundary="%s"',0 ; DATA XREF: sub_50
00504A3F 00                           align 4
00504A40 0D 0A 50 62 61 67+gibberish2 db 0Dh,0Ah            ; DATA XREF: sub_508F7D
00504A40 72 61 67 2D 47 6C+           db 'Pbagrag-Glcr: zhygvcneg/zvkrq;',0Dh,0Ah,0
00504A63 00                           align 4
00504A64 0D 0A 5A 56 5A 52+gibberish1 db 0Dh,0Ah            ; DATA XREF: sub_508F7D
00504A64 2D 49 72 65 66 76+           db 'ZVZR-Irefvba: 1.0',0
00504A78 0D 0A 51 6E 67 72+aQngr db 0Dh,0Ah                 ; DATA XREF: sub_508F7D
00504A78 3A 20 00                     db 'Qngr: ',0
00504A81 00 00 00                     align 4
```

IDA View-A

```
0050901E 03
00509020 50
00509021 E8
00509026 59
00509027 59
00509028 56
00509029 FF
0050902B 03
0050902D 50
0050902E 6A
00509030 E8
00509035 59
00509036 59                           pop ecx
00509037 68 64 4A 50 00               push offset gibberish1  ; "\r\nZVZR-Irefvba:
0050903C 56                           push esi                ; lpString
0050903D FF D7                        call edi ; lstrlenA
0050903F 03 C6                        add eax, esi
00509041 50                           push eax
00509042 E8 72 CC FF FF               call decrypt
00509047 59                           pop ecx
00509048 59                           pop ecx
00509049 68 40 4A 50 00               push offset gibberish2  ; "\r\nPbagrag-Glcr:
0050904E 56                           push esi                ; lpString
0050904F FF D7                        call edi ; lstrlenA
00509051 03 C6                        add eax, esi
00509053 50                           push eax
00509054 E8 60 CC FF F
00509059 FF 74 24 18
0050905D 68 30 4A 50 0
00509062 56
00509063 E8 B7 CB FF F
00509068 83 C4 14
0050906B 68 20 4A 50 0
00509070 56
00509071 FF D7
00509073 03 C6
00509075 50
00509076 E8 3E CC FF F
0050907B 59
0050907C 59
0050907D 68 04 4A 50 0
00509082 56
00509083 FF D7
00509085 03 C6
00509087 50
00509088 E8 2C CC FF F
0050908D 59
0050908E 59
0050908F 68 FC 49 50 0
00509094 56
00509095 FF D5
00509097 5F
00509098 5E
00509099 5D
```

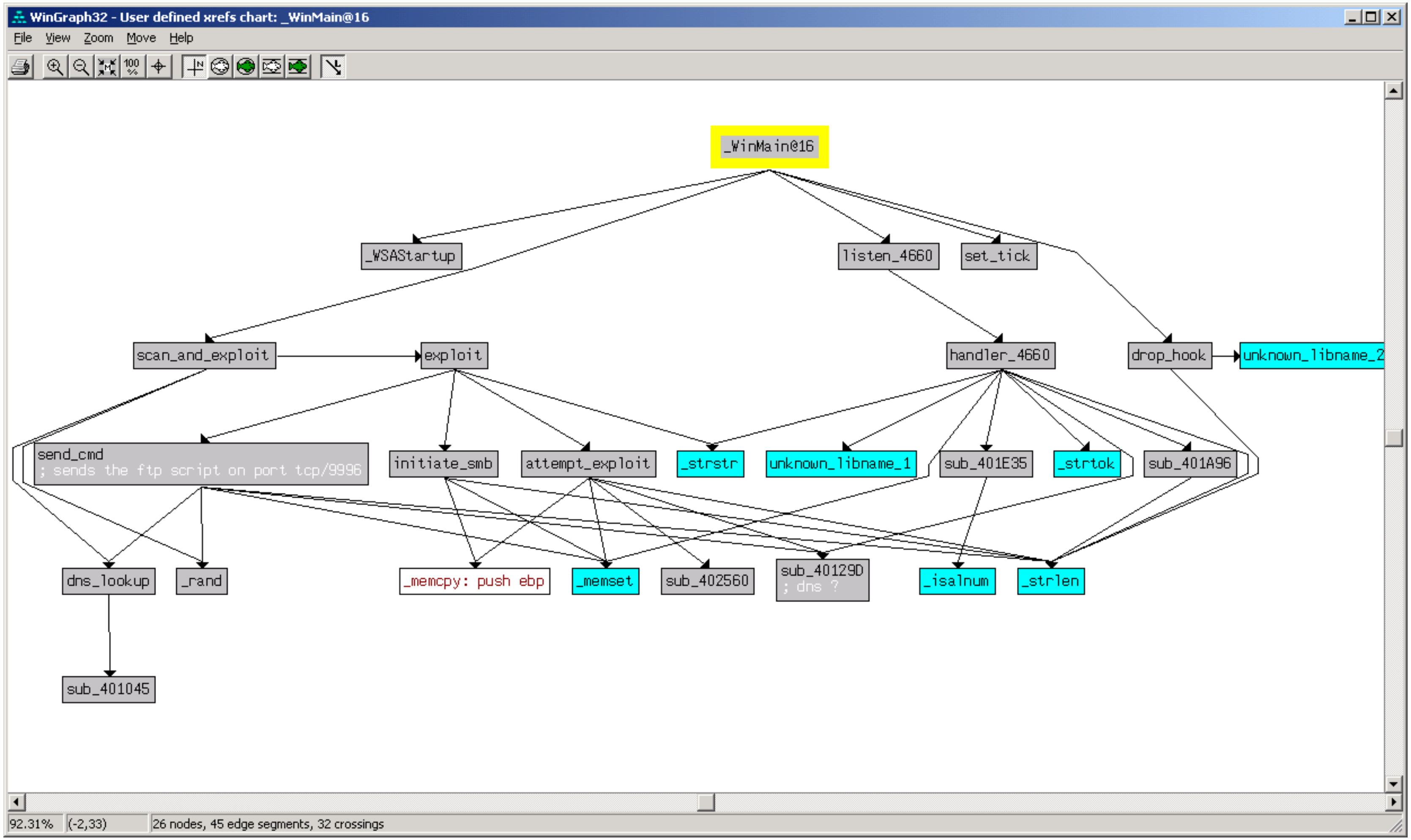
IDA View-C

```
00505CB9             decrypt proc near                      ; CODE XREF: s
00505CB9                                                    ; sub_508F7D+4
00505CB9
00505CB9             arg_0 = dword ptr  8
00505CB9             arg_4 = dword ptr  0Ch
00505CB9
00505CB9 56                  push esi
00505CBA 8B 74 24 0C         mov esi, [esp+arg_4]
00505CBE 57                  push edi
00505CBF 8B 7C 24 0C         mov edi, [esp+4+arg_0]
00505CC3
00505CC3             loc_505CC3:                            ; CODE XREF: d
00505CC3 8A 06               mov al, [esi]
00505CC5 84 C0               test al, al
00505CC7 74 0D               jz short loc_505CD6
00505CC9 50                  push eax
00505CCA E8 6F FF FF FF      call rot13
00505CCF 88 07               mov [edi], al
00505CD1 47                  inc edi
00505CD2 59                  pop ecx
00505CD3 46                  inc esi
00505CD4 EB ED               jmp short loc_505CC3
00505CD6             ; ───────────────────────────────────────
00505CD6
00505CD6             loc_505CD6:                            ; CODE XREF: d
00505CD6 80 27 00            and byte ptr [edi], 0
00505CD9 5F                  pop edi
00505CDA 5E                  pop esi
00505CDB C3                  retn
00505CDB             decrypt endp
```

```
The initial autoanalysis is finished.
Flushing buffers, please wait...ok
```

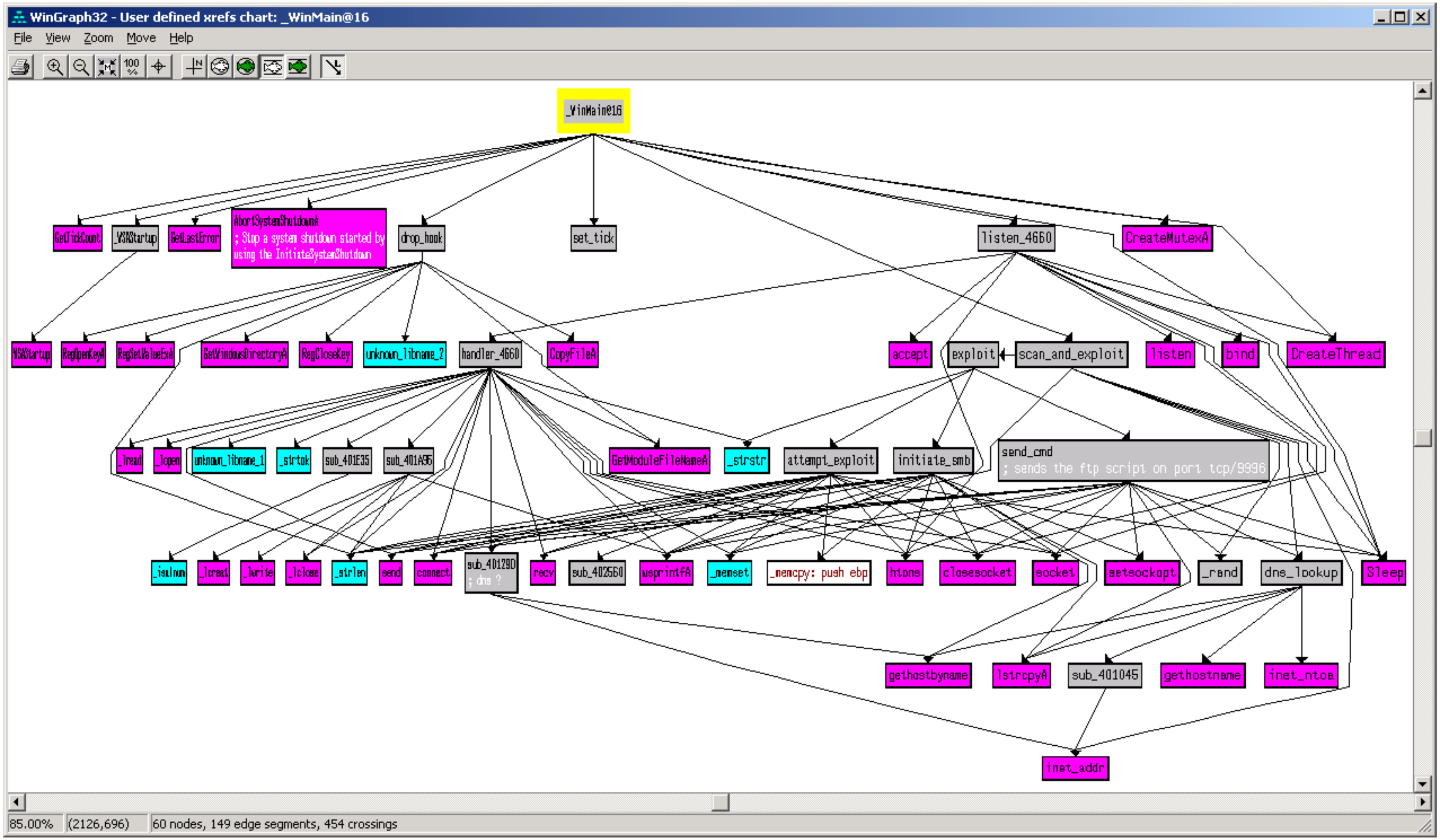
AU: idle | Down | Disk: 6GB | 00008442 | 00509042: sub_508F7D+C5

Structure of most malware is simple

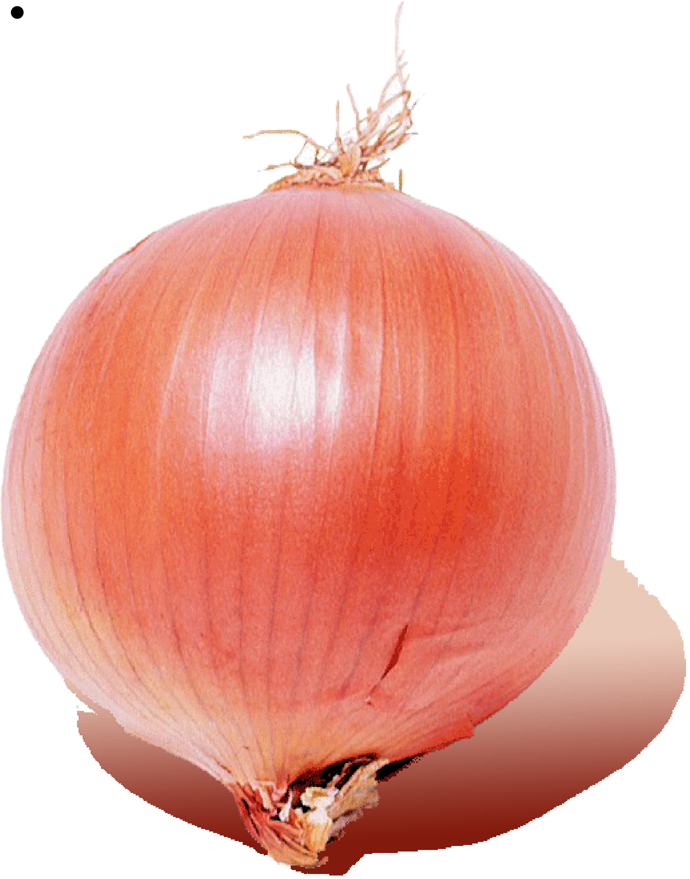


92.31% (-2,33) 26 nodes, 45 edge segments, 32 crossings

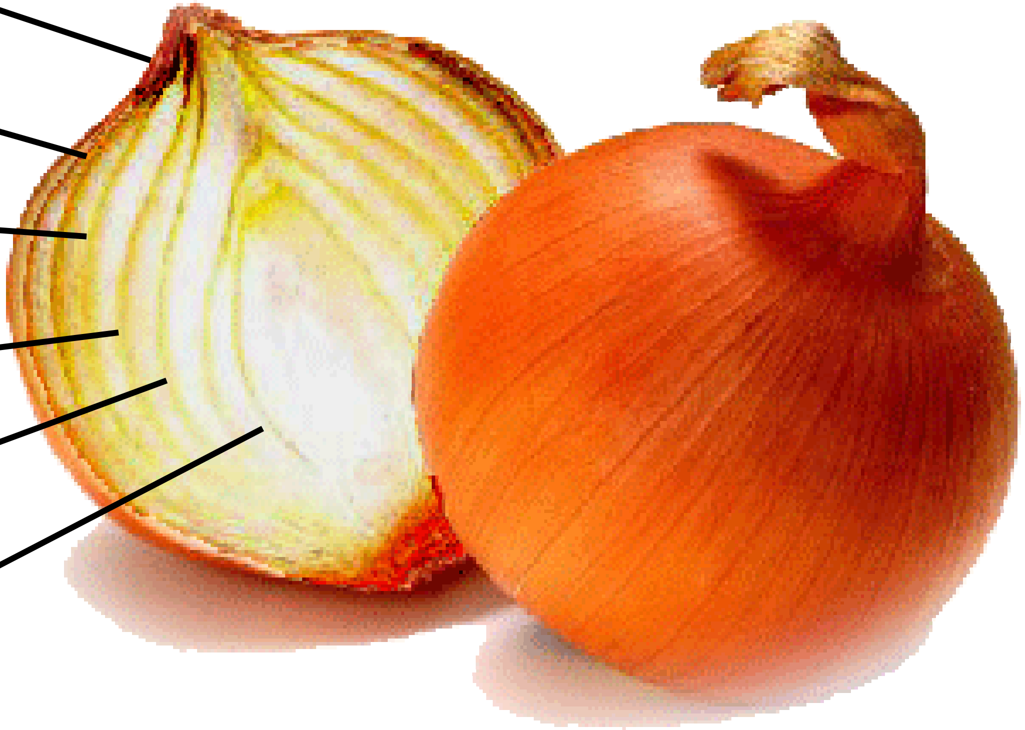
Module behaviour can be inferred



Analysis can bring a tear to your eye!



Analysis can bring a tear to your eye!



Email Headers

Base64 body

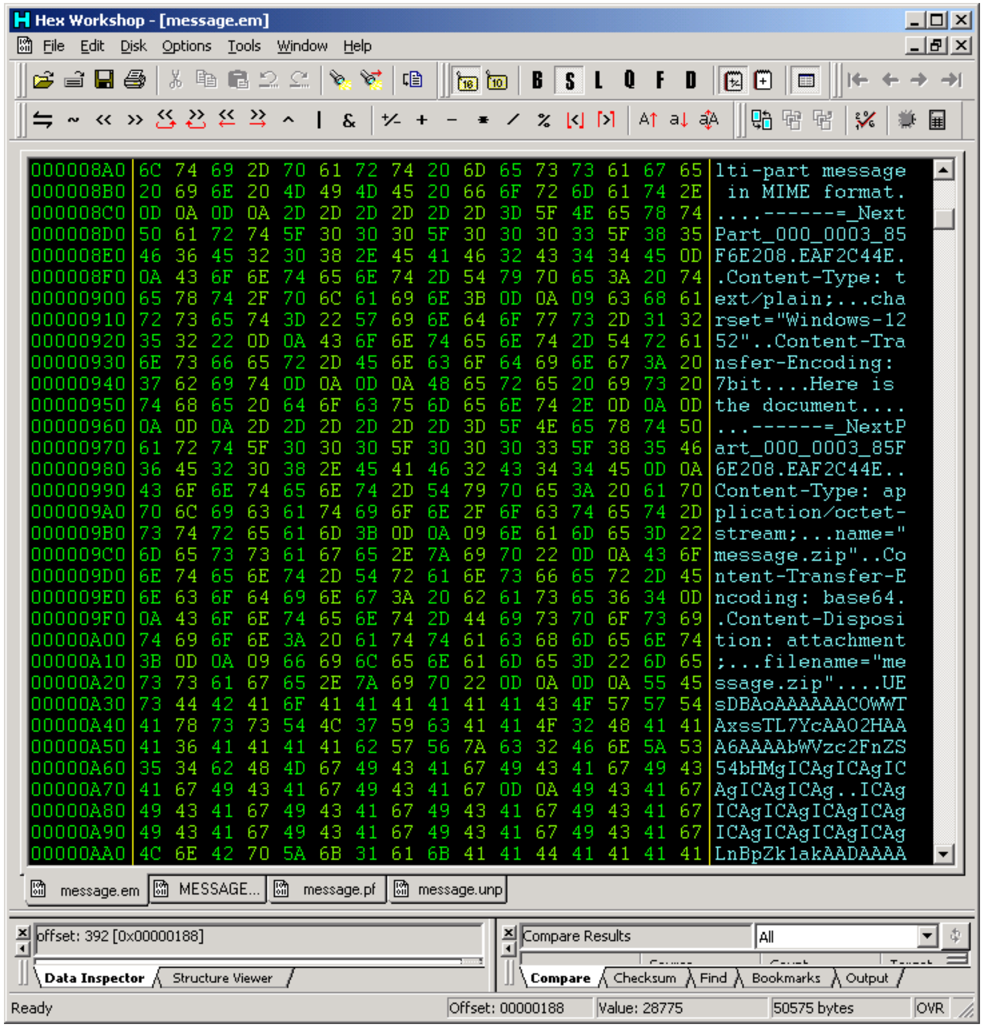
Zip Header

MZ+PE Header

Unpacking code

Core Program

Brief Example

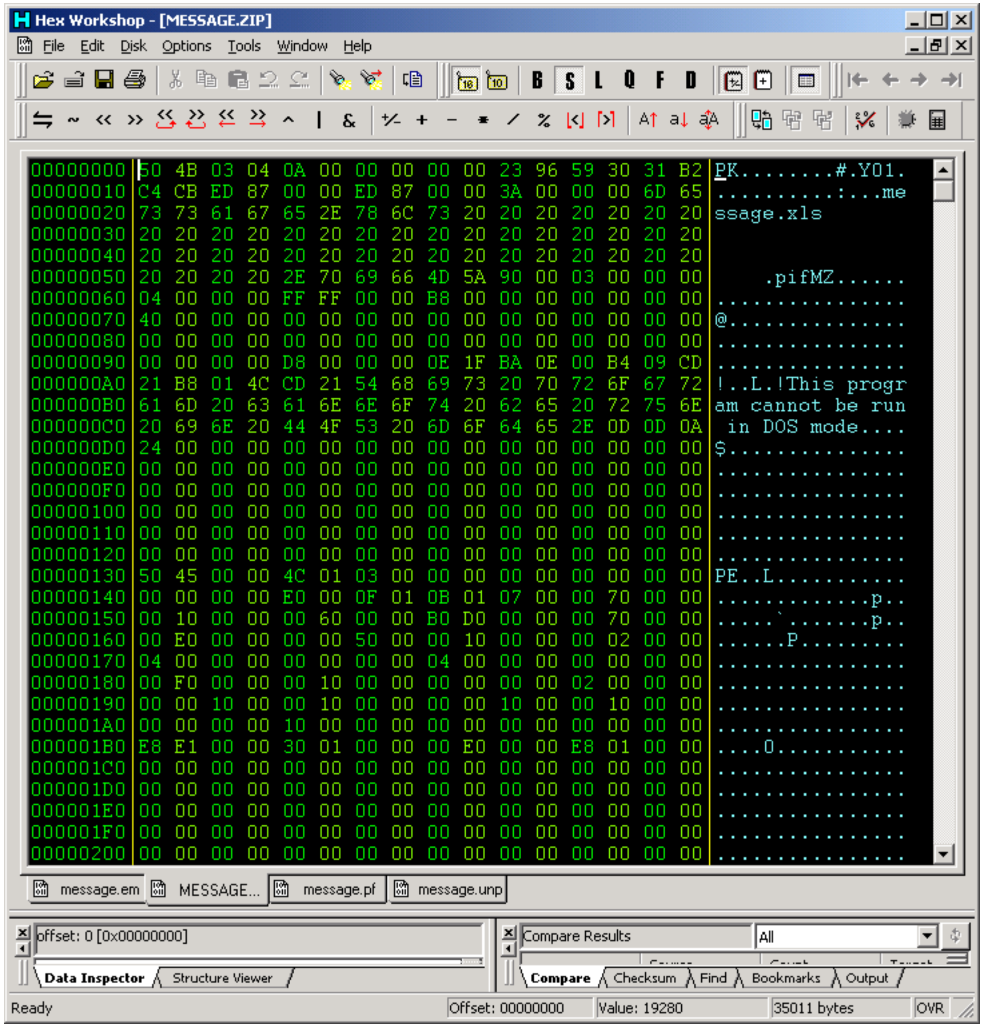


```
000008A0 6C 74 69 2D 70 61 72 74 20 6D 65 73 73 61 67 65 lti-part message
000008B0 20 69 6E 20 4D 49 4D 45 20 66 6F 72 6D 61 74 2E  in MIME format.
000008C0 0D 0A 0D 0A 2D 2D 2D 2D 2D 2D 3D 5F 4E 65 78 74 ....------=_Next
000008D0 50 61 72 74 5F 30 30 30 5F 30 30 30 33 5F 38 35 Part_000_0003_85
000008E0 46 36 45 32 30 38 2E 45 41 46 32 43 34 34 45 0D F6E208.EAF2C44E.
000008F0 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 .Content-Type: t
00000900 65 78 74 2F 70 6C 61 69 6E 3B 0D 0A 09 63 68 61 ext/plain;...cha
00000910 72 73 65 74 3D 22 57 69 6E 64 6F 77 73 2D 31 32 rset="Windows-12
00000920 35 32 22 0D 0A 43 6F 6E 74 65 6E 74 2D 54 72 61 52"..Content-Tra
00000930 6E 73 66 65 72 2D 45 6E 63 6F 64 69 6E 67 3A 20 nsfer-Encoding: 
00000940 37 62 69 74 0D 0A 0D 0A 48 65 72 65 20 69 73 20 7bit....Here is 
00000950 74 68 65 20 64 6F 63 75 6D 65 6E 74 2E 0D 0A 0D the document....
00000960 0A 0D 0A 2D 2D 2D 2D 2D 2D 3D 5F 4E 65 78 74 50 ...------=_NextP
00000970 61 72 74 5F 30 30 30 5F 30 30 30 33 5F 38 35 46 art_000_0003_85F
00000980 36 45 32 30 38 2E 45 41 46 32 43 34 34 45 0D 0A 6E208.EAF2C44E..
00000990 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 Content-Type: ap
000009A0 70 6C 69 63 61 74 69 6F 6E 2F 6F 63 74 65 74 2D plication/octet-
000009B0 73 74 72 65 61 6D 3B 0D 0A 09 6E 61 6D 65 3D 22 stream;...name="
000009C0 6D 65 73 73 61 67 65 2E 7A 69 70 22 0D 0A 43 6F message.zip"..Co
000009D0 6E 74 65 6E 74 2D 54 72 61 6E 73 66 65 72 2D 45 ntent-Transfer-E
000009E0 6E 63 6F 64 69 6E 67 3A 20 62 61 73 65 36 34 0D ncoding: base64.
000009F0 0A 43 6F 6E 74 65 6E 74 2D 44 69 73 70 6F 73 69 .Content-Disposi
00000A00 74 69 6F 6E 3A 20 61 74 74 61 63 68 6D 65 6E 74 tion: attachment
00000A10 3B 0D 0A 09 66 69 6C 65 6E 61 6D 65 3D 22 6D 65 ;...filename="me
00000A20 73 73 61 67 65 2E 7A 69 70 22 0D 0A 0D 0A 55 45 ssage.zip"....UE
00000A30 73 44 42 41 6F 41 41 41 41 41 41 43 4F 57 57 54 sDBAoAAAAAACOWWT
00000A40 41 78 73 73 54 4C 37 59 63 41 41 4F 32 48 41 41 AxssTL7YcAAO2HAA
00000A50 41 36 41 41 41 41 62 57 56 7A 63 32 46 6E 5A 53 A6AAAAbWVzc2FnZS
00000A60 35 34 62 48 4D 67 49 43 41 67 49 43 41 67 49 43 54bHMgICAgICAgIC
00000A70 41 67 49 43 41 67 49 43 41 67 0D 0A 49 43 41 67 AgICAgICAg..ICAg
00000A80 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 ICAgICAgICAgICAg
00000A90 49 43 41 67 49 43 41 67 49 43 41 67 49 43 41 67 ICAgICAgICAgICAg
00000AA0 4C 6E 42 70 5A 6B 31 61 6B 41 41 44 41 41 41 41 LnBpZk1akAADAAAA
```

offset: 392 [0x00000188]

Ready | Offset: 00000188 | Value: 28775 | 50575 bytes | OVR

Brief Example



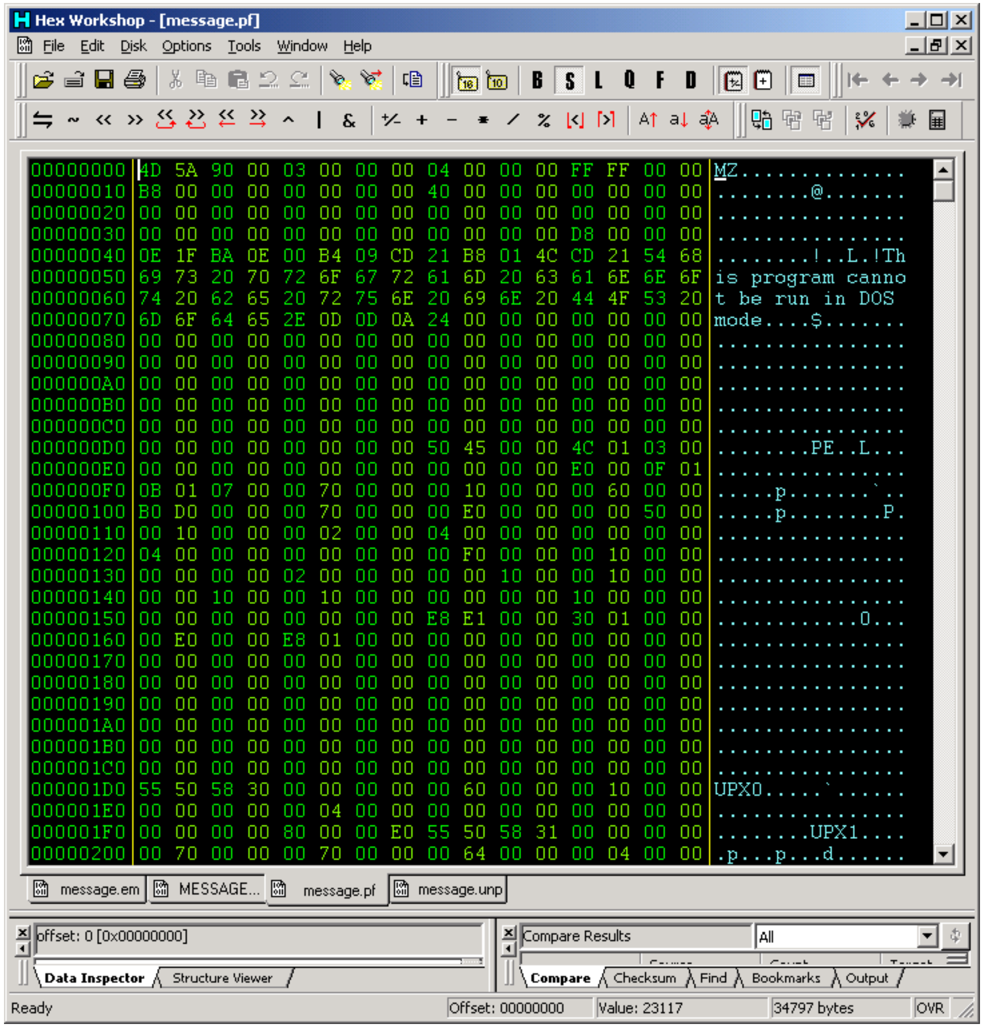
```
00000000 50 4B 03 04 0A 00 00 00 00 00 23 96 59 30 31 B2 PK........#.Y01.
00000010 C4 CB ED 87 00 00 ED 87 00 00 3A 00 00 00 6D 65 ..........:...me
00000020 73 73 61 67 65 2E 78 6C 73 20 20 20 20 20 20 20 ssage.xls
00000030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000040 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000050 20 20 20 20 2E 70 69 66 4D 5A 90 00 03 00 00 00     .pifMZ......
00000060 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 ................
00000070 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 @...............
00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000090 00 00 00 00 D8 00 00 00 0E 1F BA 0E 00 B4 09 CD ................
000000A0 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 !..L.!This progr
000000B0 61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E am cannot be run
000000C0 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A  in DOS mode....
000000D0 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 $...............
000000E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 ................
00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000130 50 45 00 00 4C 01 03 00 00 00 00 00 00 00 00 00 PE..L...........
00000140 00 00 00 00 E0 00 0F 01 0B 01 07 00 00 70 00 00 .............p..
00000150 00 10 00 00 00 60 00 00 B0 D0 00 00 00 70 00 00 .....`.......p..
00000160 00 E0 00 00 00 00 50 00 00 10 00 00 00 02 00 00 ......P.........
00000170 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 ................
00000180 00 F0 00 00 00 10 00 00 00 00 00 00 02 00 00 00 ................
00000190 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 ................
000001A0 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 ................
000001B0 E8 E1 00 00 30 01 00 00 00 E0 00 00 E8 01 00 00 ....0...........
000001C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

offset: 0 [0x00000000]

Ready | Offset: 00000000 | Value: 19280 | 35011 bytes | OVR

RuxCon 2004

Brief Example



Hex Workshop - [message.pf]
File Edit Disk Options Tools Window Help

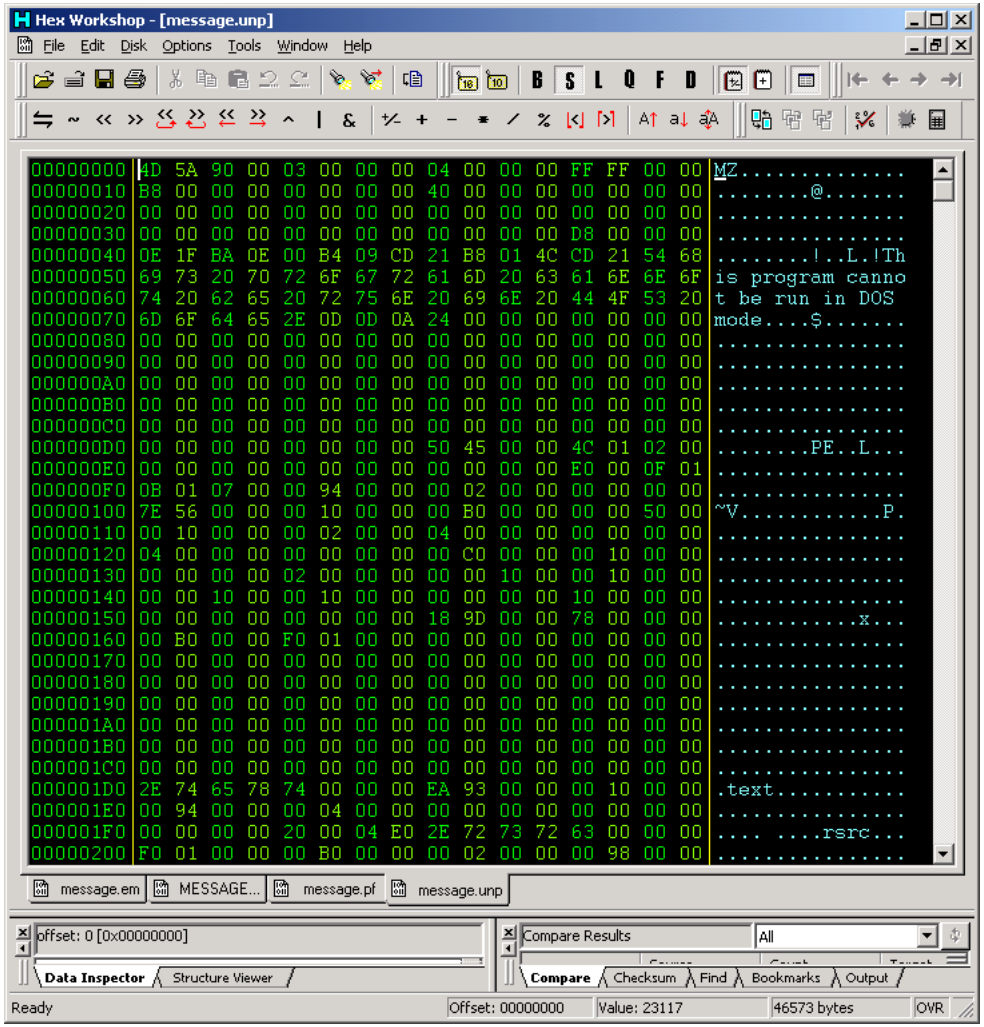
```
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ..............
00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ........@.......
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000030 00 00 00 00 00 00 00 00 00 00 00 00 D8 00 00 00 ................
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ........!..L.!Th
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS 
00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000000A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000000B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000000C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000000D0 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 03 00 ........PE..L...
000000E0 00 00 00 00 00 00 00 00 00 00 00 00 E0 00 0F 01 ................
000000F0 0B 01 07 00 00 70 00 00 00 10 00 00 00 60 00 00 .....p.......`..
00000100 B0 D0 00 00 00 70 00 00 00 E0 00 00 00 00 50 00 .....p........P.
00000110 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 ................
00000120 04 00 00 00 00 00 00 00 00 F0 00 00 00 10 00 00 ................
00000130 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 ................
00000140 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 ................
00000150 00 00 00 00 00 00 00 00 E8 E1 00 00 30 01 00 00 ............0...
00000160 00 E0 00 00 E8 01 00 00 00 00 00 00 00 00 00 00 ................
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001D0 55 50 58 30 00 00 00 00 00 60 00 00 00 10 00 00 UPX0.....`......
000001E0 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 ................
000001F0 00 00 00 00 80 00 00 E0 55 50 58 31 00 00 00 00 ........UPX1....
00000200 00 70 00 00 00 70 00 00 00 64 00 00 00 04 00 00 .p...p...d......
```

offset: 0 [0x00000000]

Ready | Offset: 00000000 | Value: 23117 | 34797 bytes | OVR

RuxCon 2004

Brief Example



Hex Workshop - [message.unp]
File Edit Disk Options Tools Window Help
B S L Q F D

```
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ..............
00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ........@.......
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000030 00 00 00 00 00 00 00 00 00 00 00 00 D8 00 00 00 ................
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ........!..L.!Th
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS 
00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000000A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000000B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000000C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000000D0 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 02 00 ........PE..L...
000000E0 00 00 00 00 00 00 00 00 00 00 00 00 E0 00 0F 01 ................
000000F0 0B 01 07 00 00 94 00 00 00 02 00 00 00 00 00 00 ................
00000100 7E 56 00 00 00 10 00 00 00 B0 00 00 00 00 50 00 ~V............P.
00000110 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 ................
00000120 04 00 00 00 00 00 00 00 00 C0 00 00 00 10 00 00 ................
00000130 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 ................
00000140 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 ................
00000150 00 00 00 00 00 00 00 00 18 9D 00 00 78 00 00 00 ............x...
00000160 00 B0 00 00 F0 01 00 00 00 00 00 00 00 00 00 00 ................
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001D0 2E 74 65 78 74 00 00 00 EA 93 00 00 00 10 00 00 .text...........
000001E0 00 94 00 00 00 04 00 00 00 00 00 00 00 00 00 00 ................
000001F0 00 00 00 00 20 00 04 E0 2E 72 73 72 63 00 00 00 .... ....rsrc...
00000200 F0 01 00 00 00 B0 00 00 00 02 00 00 00 98 00 00 ................
```

offset: 0 [0x00000000]

Ready | Offset: 00000000 | Value: 23117 | 46573 bytes | OVR

In Conclusion

- Malware analysis is focused on identifying malicious modules and documenting behaviour in a timely fashion at the expense of detailed source reconstruction.
- Although the fundamental techniques remain the same, their application is somewhat reactionary toward the sample at hand.
- It is only through laborious analysis of many samples that one begins to notice patterns and trends which can be used to refine the analysis process.

Questions ?