Macintosh OSX Binary Malware

Marius van Oers
McAfee Avert

Program

1 - Introduction
2 - Mach Header
3 - Segments
4 - Sections
5 - EP - Possible Virus Techniques
6 - Universal Binaries
7 - Tools
8 - Conclusion
9 - Questions

McAfee

1- Introduction

McAfee

Introduction

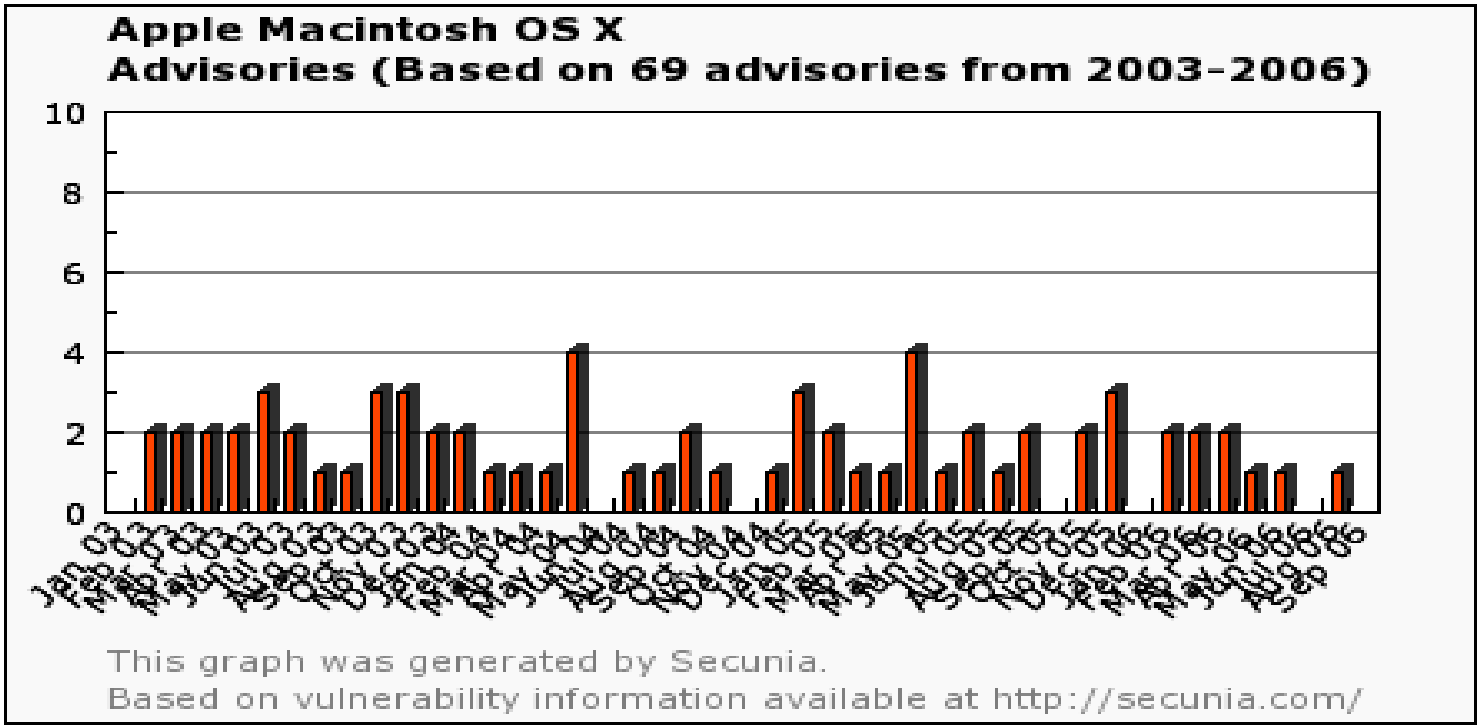
- Growing Popularity

  Mac Mini, MacBook Pro

- OSX threats Leap (binary) and Inqtana (java).

  Macintosh vulnerable to native malware?

McAfee



2003	2004	2005	2006
23	15	22	9

Source: http://secunia.com

McAfee

- NEW McAfee drivers for Macintosh
- HyperCard Script requires additional install

	2000	2001	2002	2003	2004	2005	2006
MacOS	0	10	43	12	4	0	0
MacHC	0	1	4	3	0	0	0
OSX	0	0	0	0	0	1	5

McAfee

- Malware Numbers:

MacOS-HC-OSX	LINUX-UNIX	WINDOWS
83	700	212.000

- Macintosh MarketShare 5%
- User/Root rights
- Open Source

Architecture

- PowerPC ←→ INTEL
- MSB ←→ LSB
- 64 BIT ←→ 32 BIT
- Applications with Universal symbol run on both

- Mach-O (Mach object) Binary format.
  OSX/Leap examined at binary level

McAfee

OSX/Leap

latestpics

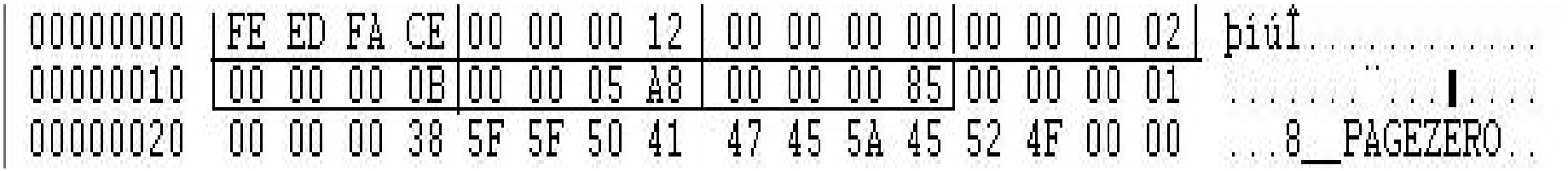
```
00000000  FE ED FA CE 00 00 00 12  00 00 00 00 00 00 00 02  þíúÎ............
00000010  00 00 00 0B 00 00 05 A8  00 00 00 85 00 00 00 01  ...........¨....
00000020  00 00 00 38 5F 5F 50 41  47 45 5A 45 52 4F 00 00  ...8__PAGEZERO..
00000030  00 00 00 00 00 00 00 00  00 00 10 00 00 00 00 00  ................
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000050  00 00 00 04 00 00 00 01  00 00 01 8C 5F 5F 54 45  ............__TE
00000060  58 54 00 00 00 00 00 00  00 00 00 00 00 00 10 00  XT..............
00000070  00 00 30 00 00 00 00 00  00 00 30 00 00 00 00 07  ..0.......0.....
00000080  00 00 00 05 00 00 00 05  00 00 00 00 5F 5F 74 65  ............__te
00000090  78 74 00 00 00 00 00 00  00 00 00 00 5F 5F 54 45  xt..........__TE
000000A0  58 54 00 00 00 00 00 00  00 00 00 00 00 00 23 44  XT............#D
000000B0  00 00 12 68 00 00 13 44  00 00 00 02 00 00 00 00  ...h...D........
000000C0  00 00 00 00 80 00 04 00  00 00 00 00 00 00 00 00  ....¨...........
000000D0  5F 5F 70 69 63 73 79 6D  62 6F 6C 5F 73 74 75 62  __picsymbol_stub
000000E0  5F 5F 54 45 58 54 00 00  00 00 00 00 00 00 00 00  __TEXT..........
000000F0  00 00 35 AC 00 00 00 00  00 00 25 AC 00 00 00 02  ..5¬......%¬....
00000100  00 00 00 00 00 00 00 00  80 00 00 08 00 00 00 00  ........¨.......
00000110  00 00 00 24 5F 5F 73 79  6D 62 6F 6C 5F 73 74 75  ...$__symbol_stu
00000120  62 00 00 00 5F 5F 54 45  58 54 00 00 00 00 00 00  b...__TEXT......
00000130  00 00 00 00 00 00 35 AC  00 00 00 00 00 00 25 AC  ......5¬......%¬
00000140  00 00 00 02 00 00 00 00  00 00 00 00 80 00 00 08  ............¨...
00000150  00 00 00 00 00 00 00 14  5F 5F 70 69 63 73 79 6D  ........__picsym
00000160  62 6F 6C 73 74 75 62 31  5F 5F 54 45 58 54 00 00  bolstub1__TEXT..
00000170  00 00 00 00 00 00 00 00  00 00 35 C0 00 00 05 80  ..........5À...¨
00000180  00 00 25 C0 00 00 00 05  00 00 00 00 00 00 00 00  ..%À............
00000190  80 00 04 08 00 00 00 00  00 00 00 20 5F 5F 63 73  ¨..........  __cs
000001A0  74 72 69 6E 67 00 00 00  00 00 00 00 5F 5F 54 45  tring.....__TE
000001B0  58 54 00 00 00 00 00 00  00 00 00 00 00 00 3B 40  XT............;@
000001C0  00 00 04 84 00 00 2B 40  00 00 00 02 00 00 00 00  ...¨..+@........
000001D0  00 00 00 00 00 00 00 02  00 00 00 00 00 00 00 00  ................
000001E0  00 00 00 01 00 00 01 D0  5F 5F 44 41 54 41 00 00  .......Ð__DATA..
000001F0  00 00 00 00 00 00 00 00  00 00 40 00 00 00 50 00  ..........@...P.
00000200  00 00 30 00 00 00 50 00  00 00 00 07 00 00 00 03  ..0...P.........
```

McAfee

2- Mach Header

McAfee

Mach Header



- magic : FEEDFACE - Mach-O file
- cputype : 12 PPC
- cpusubtype : 0 ALL
- filetype : 2 EXECUTABLE
- ncmds : B
- sizeofcmds : 5A8
- flags : 85

- MSB – 32 - EP

McAfee

CpuType

- machine.h

VAX	1	1 (Hex)
MC680x0	6	6
I386	7	**7**
MC98000	10	A
HPPA	11	B
MC88000	13	D
SPARC	14	E
I860	15	F
POWERPC	18	**12**

FileType

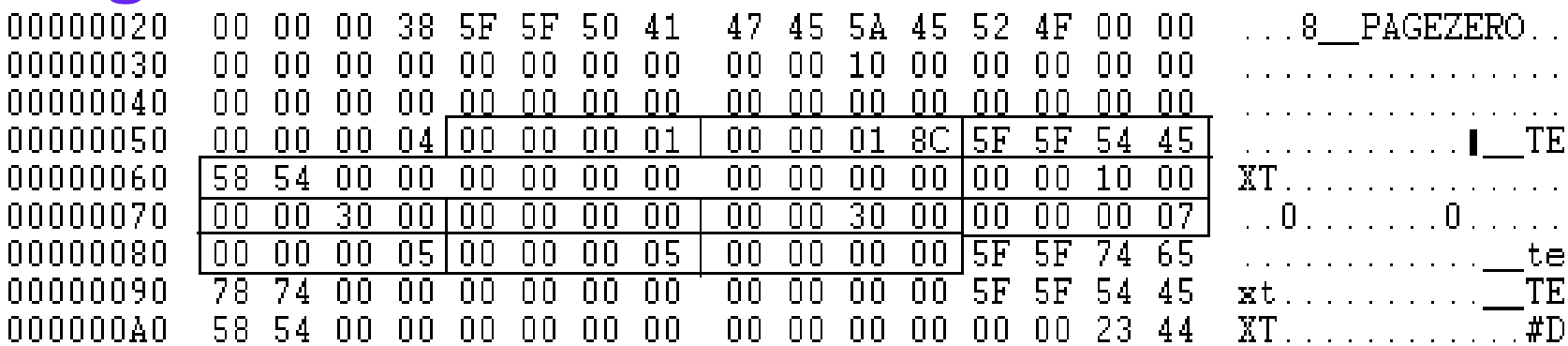
1	relocatable object file
2	demand paged executable file
3	fixed VM shared library file
4	core file
5	preloaded executable file
6	dynamically bound shared library
7	dynamic link editor
8	dynamically bound bundle file
9	shared library stub for static linking only, no section contents

McAfee

3- Segments

McAfee

Segments

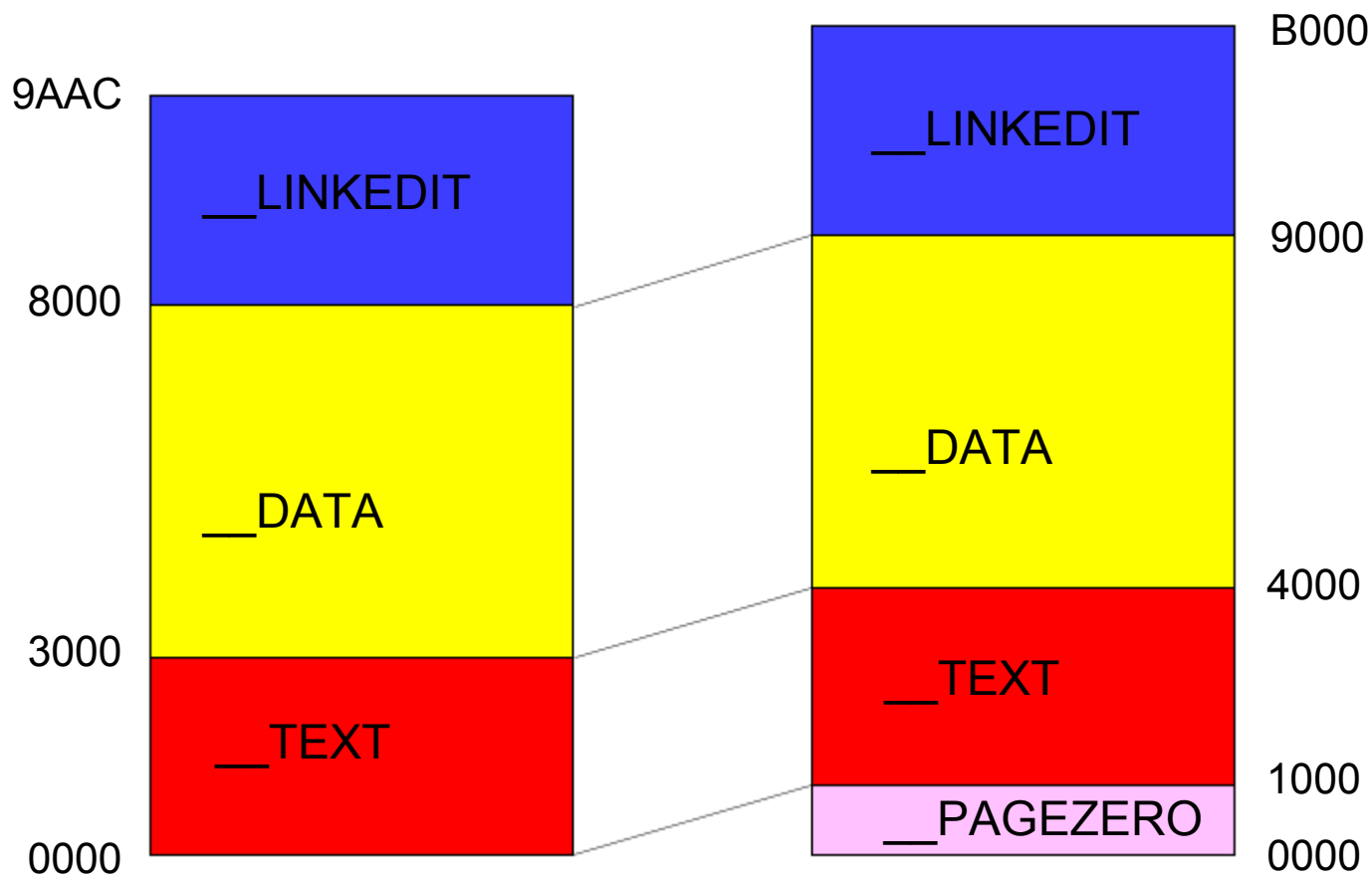


```
00000020  00 00 00 38 5F 5F 50 41  47 45 5A 45 52 4F 00 00   ...8__PAGEZERO..
00000030  00 00 00 00 00 00 00 00  00 00 10 00 00 00 00 00   ................
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000050  00 00 00 04 00 00 00 01  00 00 01 8C 5F 5F 54 45   ............__TE
00000060  58 54 00 00 00 00 00 00  00 00 00 00 00 00 10 00   XT..............
00000070  00 00 30 00 00 00 00 00  00 00 30 00 00 00 00 07   ..0.......0.....
00000080  00 00 00 05 00 00 00 05  00 00 00 00 5F 5F 74 65   ............__te
00000090  78 74 00 00 00 00 00 00  00 00 00 00 5F 5F 54 45   xt..........__TE
000000A0  58 54 00 00 00 00 00 00  00 00 00 00 00 00 23 44   XT............#D
```

- cmd : 1
- cmdsize : 18C
- segname : __TEXT the name field has 0x10 bytes allocated
- vmaddr : 1000 starting virtual memory address
- vmsize : 3000 number of bytes in virtual memory
- fileoff : 0 offset in file of the data to be mapped at vmaddr
- filesize : 3000 number of bytes occupied by this segment on disk
- maxprot : 7 maximum permitted virtual memory protections
- initprot : 5 initial virtual memory protections
- nsects : 5 the number of section data structures following this load command.
- flags : 0

McAfee

File and Virtual Memory Area for the 4 segments



McAfee

Nsects

cmdsize	38	18C	1D0	38
segname	__PAGEZERO	__TEXT	__DATA	__LINKEDIT
nsects	0	5	6	0

McAfee

4- Sections

McAfee

Sections

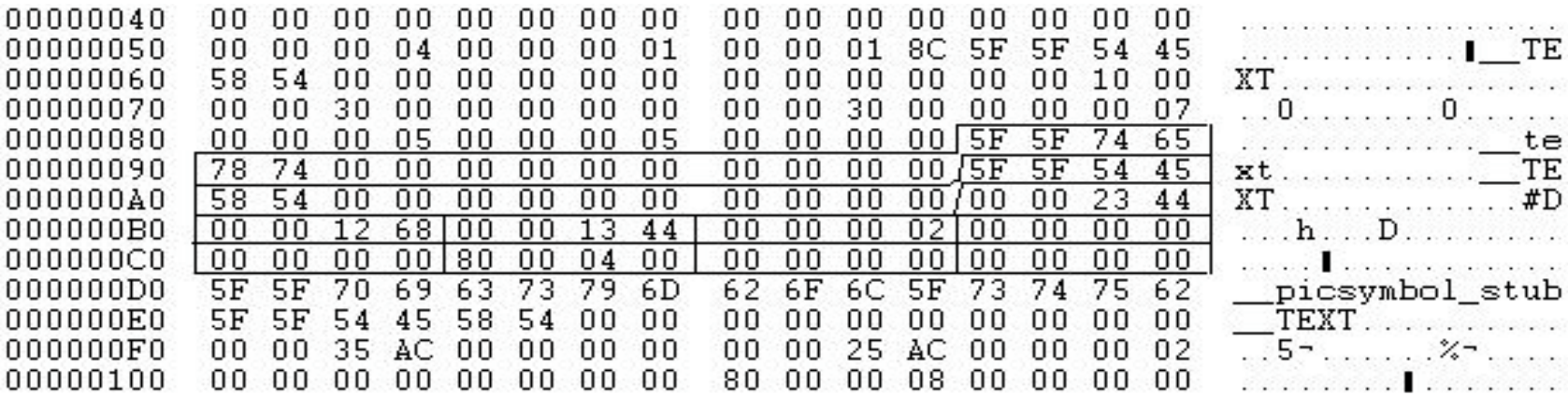
latestpics

```
00000000  FE ED FA CE 00 00 00 12  00 00 00 00 00 00 00 02  þíúÎ............
00000010  00 00 00 0B 00 00 05 A8  00 00 00 85 00 00 00 01  ...........¨....
00000020  00 00 00 38 5F 5F 50 41  47 45 5A 45 52 4F 00 00  ...8__PAGEZERO..
00000030  00 00 00 00 00 00 00 00  00 00 10 00 00 00 00 00  ................
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000050  00 00 00 04 00 00 00 01  00 00 01 8C 5F 5F 54 45  ............__TE
00000060  58 54 00 00 00 00 00 00  00 00 00 00 00 00 10 00  XT..............
00000070  00 00 30 00 00 00 00 00  00 00 30 00 00 00 00 07  ..0.......0.....
00000080  00 00 00 05 00 00 00 05  00 00 00 00 5F 5F 74 65  ............__te
00000090  78 74 00 00 00 00 00 00  00 00 00 00 5F 5F 54 45  xt..........__TE
000000A0  58 54 00 00 00 00 00 00  00 00 00 00 00 00 23 44  XT............#D
000000B0  00 00 12 68 00 00 13 44  00 00 00 02 00 00 00 00  ...h...D........
000000C0  00 00 00 00 80 00 04 00  00 00 00 00 00 00 00 00  ....¬...........
000000D0  5F 5F 70 69 63 73 79 6D  62 6F 6C 5F 73 74 75 62  __picsymbol_stub
000000E0  5F 5F 54 45 58 54 00 00  00 00 00 00 00 00 00 00  __TEXT..........
000000F0  00 00 35 AC 00 00 00 00  00 00 25 AC 00 00 00 02  ..5¬......%¬....
00000100  00 00 00 00 00 00 00 00  80 00 00 08 00 00 00 00  ........¬.......
00000110  00 00 00 24 5F 5F 73 79  6D 62 6F 6C 5F 73 74 75  ...$__symbol_stu
00000120  62 00 00 00 5F 5F 54 45  58 54 00 00 00 00 00 00  b...__TEXT......
00000130  00 00 00 00 00 00 35 AC  00 00 00 00 00 00 25 AC  ......5¬......%¬
00000140  00 00 00 02 00 00 00 00  00 00 00 00 80 00 00 08  ............¬...
00000150  00 00 00 00 00 00 00 14  5F 5F 70 69 63 73 79 6D  ........__picsym
00000160  62 6F 6C 73 74 75 62 31  5F 5F 54 45 58 54 00 00  bolstub1__TEXT..
00000170  00 00 00 00 00 00 00 00  00 00 35 C0 00 00 05 80  ..........5À...¬
00000180  00 00 25 C0 00 00 00 05  00 00 00 00 00 00 00 00  ..%À............
00000190  80 00 04 08 00 00 00 00  00 00 00 20 5F 5F 63 73  ¬..........  __cs
000001A0  74 72 69 6E 67 00 00 00  00 00 00 00 00 00 5F 5F  tring.........__
000001B0  54 45 58 54 00 00 00 00  00 00 00 00 00 00 3B 40  TEXT..........;@
000001C0  00 00 04 84 00 00 2B 40  00 00 00 02 00 00 00 00  ...¬..+@........
000001D0  00 00 00 00 00 00 00 02  00 00 00 00 00 00 00 00  ................
000001E0  00 00 00 01 00 00 01 D0  5F 5F 44 41 54 41 00 00  .......Ð__DATA..
000001F0  00 00 00 00 00 00 00 00  00 00 40 00 00 00 50 00  ..........@...P.
00000200  00 00 30 00 00 00 50 00  00 00 00 07 00 00 00 03  ..0...P.........
00000210  00 00 00 06 00 00 00 00  5F 5F 64 61 74 61 00 00  ........__data..
00000220  00 00 00 00 00 00 00 00  5F 5F 44 41 54 41 00 00  ........__DATA..
00000230  00 00 00 00 00 00 00 00  00 00 40 00 00 00 49 10  ..........@...I.
```

- OSX/Leap has 5 sections inside the __TEXT segment

McAfee

__text section inside the __TEXT segment



```
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000050  00 00 00 04 00 00 00 01  00 00 01 8C 5F 5F 54 45  ............__TE
00000060  58 54 00 00 00 00 00 00  00 00 00 00 00 00 10 00  XT..............
00000070  00 00 30 00 00 00 00 00  00 00 30 00 00 00 00 07  ..0.......0.....
00000080  00 00 00 05 00 00 00 05  00 00 00 00 5F 5F 74 65  ............__te
00000090  78 74 00 00 00 00 00 00  00 00 00 00 5F 5F 54 45  xt..........__TE
000000A0  58 54 00 00 00 00 00 00  00 00 00 00 00 00 23 44  XT............#D
000000B0  00 00 12 68 00 00 13 44  00 00 00 02 00 00 00 00  ...h...D........
000000C0  00 00 00 00 80 00 04 00  00 00 00 00 00 00 00 00  ................
000000D0  5F 5F 70 69 63 73 79 6D  62 6F 6C 5F 73 74 75 62  __picsymbol_stub
000000E0  5F 5F 54 45 58 54 00 00  00 00 00 00 00 00 00 00  __TEXT..........
000000F0  00 00 35 AC 00 00 00 00  00 00 25 AC 00 00 00 02  ..5¬......%¬....
00000100  00 00 00 00 00 00 00 00  80 00 00 08 00 00 00 00  ................
```

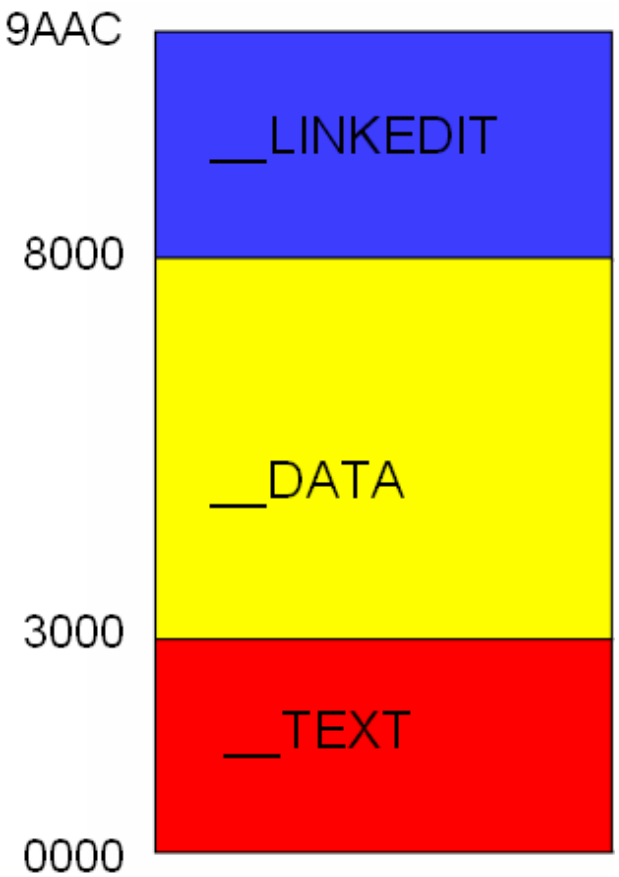
- sectname : __text , the name field has 0x10 bytes allocated
- segname : __TEXT , the name field has 0x10 bytes allocated
- addr : 2344
- size : 1268
- offset : 1344
- align : 2
- reloff : 0
- nreloc : 0
- flags : 80000400
- reserved1 : 0
- reserved2 : 0

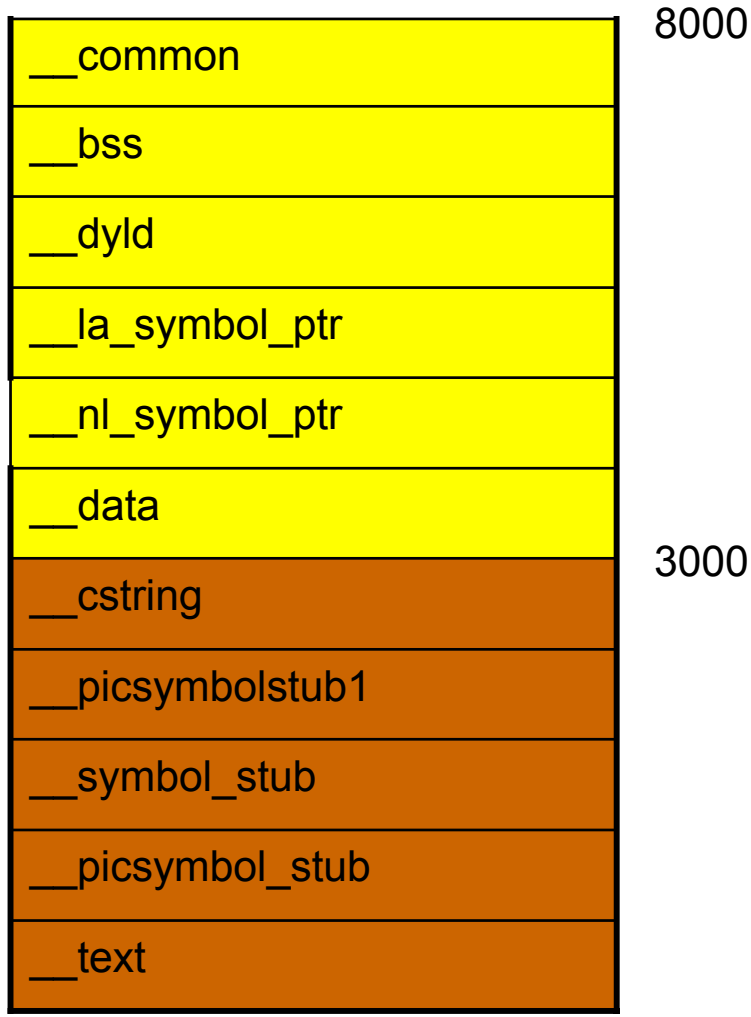
McAfee

Section command info for the various sections inside the __TEXT segment.

sectname	__text	__picsymbol_stub	__symbol_stub	__picsymbolstub1	__cstring
segname	__TEXT	__TEXT	__TEXT	__TEXT	__TEXT
addr	2344	35AC	35AC	35C0	3B40
size	**1268**	**0**	**0**	**580**	**484**
offset	**1344**	**25AC**	**25AC**	**25C0**	**2B40**
align	2	2	2	5	2
reloff	0	0	0	0	0
nreloc	0	0	0	0	0
flags	**80000400**	**80000008**	**80000008**	**80000408**	**2**
reserved1	0	0	0	0	0
reserved2	0	24	14	20	0

Section File Areas in the __TEXT and __DATA segments.





McAfee

5- EP – Possible Virus Techniques

McAfee

EP / Possible Virus Techniques

CALC.exe

```
00000000  4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00  MZ▌.........ÿÿ..
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 C8 00 00 00  ............È...
00000040  0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!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  D6 C3 38 22 92 A2 56 71  92 A2 56 71 92 A2 56 71  ÖÃ8"'¢Vq'¢Vq'¢Vq
00000090  F8 BE 54 71 89 A2 56 71  92 A2 57 71 CC A2 56 71  ø¾Tq‰¢Vq'¢WqÌ¢Vq
000000A0  F0 BD 45 71 99 A2 56 71  55 A4 50 71 93 A2 56 71  ð½Eq™¢VqU¤Pq“¢Vq
000000B0  92 A2 56 71 B9 A2 56 71  52 69 63 68 92 A2 56 71  '¢Vq¹¢VqRich'¢Vq
000000C0  00 00 00 00 00 00 00 00  50 45 00 00 4C 01 03 00  ........PE..L...
000000D0  B4 AF FD 34 00 00 00 00  00 00 00 00 E0 00 0F 03  ´¯ý4........à...
000000E0  0B 01 05 0C 00 1C 01 00  00 38 00 00 00 00 00 00  ▌.........8......
000000F0  E0 19 01 00 00 10 00 00  00 30 01 00 00 00 00 01  à.........0......
00000100  00 10 00 00 00 10 00 00  05 00 00 00 05 00 00 00  ................
00000110  04 00 00 00 00 00 00 00  00 70 01 00 00 06 00 00  .........p......
00000120  98 53 02 00 02 00 00 00  00 00 04 00 00 10 00 00  ▌S..............
00000130  00 00 10 00 00 10 00 00  00 00 00 00 10 00 00 00  ................
00000140  00 00 00 00 00 00 00 00  20 20 01 00 8C 00 00 00  ........  ..▌...
00000150  00 40 01 00 18 26 00 00  00 00 00 00 00 00 00 00  .@...&..........
00000160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000170  F0 11 00 00 1C 00 00 00  00 00 00 00 00 00 00 00  ð...............
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 10 00 00 E8 01 00 00  00 00 00 00 00 00 00 00  ....è...........
000001B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001C0  2E 74 65 78 74 00 00 00  0E 1A 01 00 00 10 00 00  .text...........
000001D0  00 20 01 00 00 10 00 00  00 00 00 00 00 00 00 00  . ..............
000001E0  00 00 00 00 20 00 00 60  2E 64 61 74 61 00 00 00  .... ..`.data...
000001F0  84 0F 00 00 00 30 01 00  00 10 00 00 00 30 01 00  ▌....0.......0..
```

- File Header
- Entrypoint
- PE Binary

McAfee

ARCH

```
00000000  7F 45 4C 46 01 01 01 00  00 00 00 00 00 00 00 00  ▌ELF............
00000010  02 00 03 00 01 00 00 00  E0 83 04 08 34 00 00 00  ........à▌..4...
00000020  4C 07 00 00 00 00 00 00  34 00 20 00 06 00 28 00  L.......4. ...(.
00000030  18 00 17 00 06 00 00 00  34 00 00 00 34 80 04 08  ........4...4▌..
00000040  34 80 04 08 C0 00 00 00  C0 00 00 00 05 00 00 00  4▌..À...À.......
00000050  04 00 00 00 03 00 00 00  F4 00 00 00 F4 80 04 08  ........ô...ô▌..
00000060  F4 80 04 08 13 00 00 00  13 00 00 00 04 00 00 00  ô▌..............
00000070  01 00 00 00 01 00 00 00  00 00 00 00 00 80 04 08  ..............▌.
00000080  00 80 04 08 8D 05 00 00  8D 05 00 00 05 00 00 00  .▌..▌...▌.......
00000090  00 10 00 00 01 00 00 00  90 05 00 00 90 95 04 08  ........▌...▌▌..
000000A0  90 95 04 08 F0 00 00 00  08 01 00 00 06 00 00 00  ▌▌..ð...........
000000B0  00 10 00 00 02 00 00 00  E0 05 00 00 E0 95 04 08  ........à...à▌..
000000C0  E0 95 04 08 A0 00 00 00  A0 00 00 00 06 00 00 00  à▌.. ... ........
000000D0  04 00 00 00 04 00 00 00  08 01 00 00 08 81 04 08  ..............▌.
000000E0  08 81 04 08 20 00 00 00  20 00 00 00 04 00 00 00  .▌.. ... ........
000000F0  04 00 00 00 2F 6C 69 62  2F 6C 64 2D 6C 69 6E 75  ..../lib/ld-linu
00000100  78 2E 73 6F 2E 32 00 00  04 00 00 00 10 00 00 00  x.so.2..........
00000110  01 00 00 00 47 4E 55 00  00 00 00 00 02 00 00 00  ....GNU.........
00000120  00 00 00 00 00 00 00 00  03 00 00 00 0A 00 00 00  ................
00000130  09 00 00 00 05 00 00 00  08 00 00 00 00 00 00 00  ................
00000140  00 00 00 00 00 00 00 00  01 00 00 00 02 00 00 00  ................
00000150  03 00 00 00 00 00 00 00  06 00 00 00 07 00 00 00  ................
00000160  04 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000170  00 00 00 00 76 00 00 00  6C 83 04 08 81 00 00 00  ....v...l▌..▌...
00000180  22 00 00 00 21 00 00 00  7C 83 04 08 76 00 00 00  "...!...|▌..v...
00000190  12 00 00 00 3D 00 00 00  8C 83 04 08 AC 00 00 00  ....=...▌▌..¬...
000001A0  22 00 00 00 37 00 00 00  9C 83 04 08 37 00 00 00  "...7...▌▌..7...
000001B0  12 00 00 00 64 00 00 00  AC 83 04 08 E1 00 00 00  ....d...¬▌..á...
000001C0  12 00 00 00 1A 00 00 00  BC 83 04 08 2E 00 00 00  ........¼▌......
000001D0  12 00 00 00 28 00 00 00  CC 83 04 08 7D 00 00 00  ....(...Ì▌..}...
000001E0  22 00 00 00 55 00 00 00  80 85 04 08 04 00 00 00  "...U...▌▌......
000001F0  11 00 0E 00 01 00 00 00  00 00 00 00 00 00 00 00  ................
```

- File Header
- Entrypoint
- ELF Binary

McAfee

Possible Virus Techniques for OSX Mach-O Files

- No EP in Mach Header
- Change the immediate bytes at the start or the end of the executable code itself in the __text section
- Or by putting a call instruction in these to another section where the real virus bytes reside.

McAfee

- *underscores__sectname = Tradition, Not Mandatory*
- *section type and attributes are important.*

Section **flags** field holds dual information about these:
least 8 bits define the section **type**.
most 24 significant bits define the section **attributes**.

If flags = 11223344 then
type = 44
attributes = 11223300

sectname	__text	
flags	80000400	
type	0	Regular section
attributes	0x80000400	Contains Machine Instructions

TYPE

REGULAR	0x0	regular section
ZEROFILL	0x1	zero fill on demand section
CSTRING_LITERALS	0x2	section with only literal C strings
NON_LAZY_SYMBOL_POINTERS	0x6	section with only non-lazy symbol pointers
LAZY_SYMBOL_POINTERS	0x7	section with only lazy symbol pointers
SYMBOL_STUBS	0x8	section with only symbol stubs, byte size of stub in

Attributes

S_ATTR_PURE_INSTRUCTIONS 0x80000000	section contains only true machine instructions
S_ATTR_SOME_INSTRUCTIONS 0x00000400	section contains some machine instructions

sectname	__text	__picsymbol_stub	__symbol_stub	__picsymbolstub1	__cstring
flags	80000400	80000008	80000008	80000408	2
type	0	8	8	8	2
attributes	0x80000400	0x80000000	0x80000000	0x8000400	0

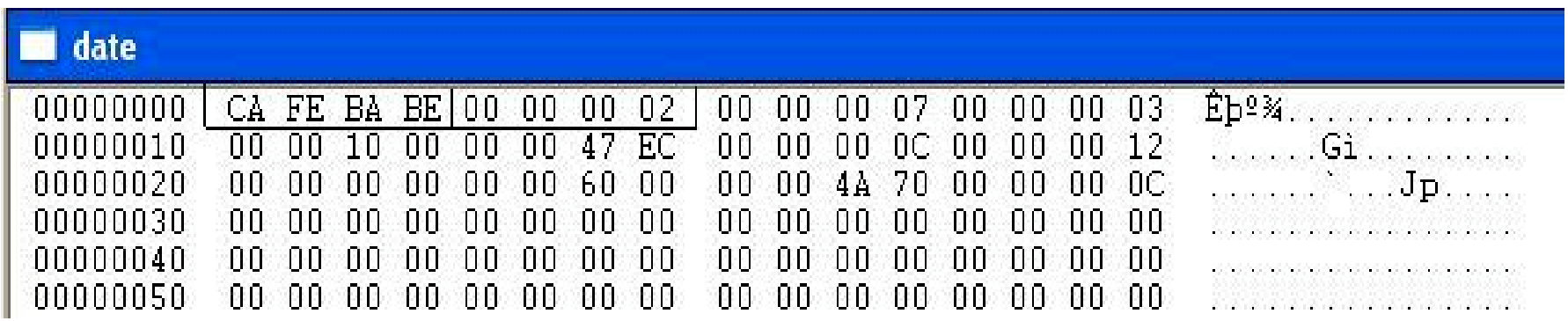
sectname	__data	__nl_symbol_ptr	__la_symbol_ptr	__dyld	__bss	__common
flags	0	6	7	0	1	1
type	0	6	7	0	1	1
attributes	0	0	0	0	0	0

6- Universal Binaries

McAfee

Universal Binaries

- **PPC/PPC64** : both 32 and 64 bit PowerPC
- **Universal Binaries** : Code for Intel + PowerPC
- **fat_header** and **fat_arch** always use Big Endian



Universal Binaries

date

```
00000000  CA FE BA BE 00 00 00 02  00 00 00 07 00 00 00 03  Êþº¾............
00000010  00 00 10 00 00 00 47 EC  00 00 00 0C 00 00 00 12  ......Gì........
00000020  00 00 00 00 00 00 60 00  00 00 4A 70 00 00 00 0C  ......`...Jp....
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000040  00 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  ................
```

date

```
00000000  CA FE BA BE 00 00 00 02  00 00 00 07 00 00 00 03  Êþº¾............
00000010  00 00 10 00 00 00 47 EC  00 00 00 0C 00 00 00 12  ......Gì........
00000020  00 00 00 00 00 00 60 00  00 00 4A 70 00 00 00 0C  ......`...Jp....
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000040  00 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  ................
```

cputype	7 (I386)	12 (PowerPC)
cpusubtype	3 (ALL)	0 (ALL)
offset	1000	6000
size	47EC	4A70
align	C	C
File Area	1000-57EC (Active code ends, filled till 6000 with zero's)	6000-AA70 (EOF)

McAfee

Universal Binaries

date

```
00000FC0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000FD0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000FE0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000FF0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00001000  CE FA ED FE 07 00 00 00  03 00 00 00 02 00 00 00  Îúíþ............
00001010  0C 00 00 00 0C 05 00 00  85 00 00 00 01 00 00 00  ........▌.......
00001020  38 00 00 00 5F 5F 50 41  47 45 5A 45 52 4F 00 00  8...__PAGEZERO..
00001030  00 00 00 00 00 00 00 00  00 10 00 00 00 00 00 00  ................
00001040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00001050  04 00 00 00 01 00 00 00  8C 01 00 00 5F 5F 54 45  ........▌...__TE
00001060  58 54 00 00 00 00 00 00  00 00 00 00 00 10 00 00  XT..............
```

date

```
00005FD0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00005FE0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00005FF0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00006000  FE ED FA CE 00 00 00 12  00 00 00 00 00 00 00 02  þíúÎ............
00006010  00 00 00 0B 00 00 05 34  00 00 00 85 00 00 00 01  .......4...▌....
00006020  00 00 00 38 5F 5F 50 41  47 45 5A 45 52 4F 00 00  ...8__PAGEZERO..
00006030  00 00 00 00 00 00 00 00  00 00 10 00 00 00 00 00  ................
00006040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00006050  00 00 00 04 00 00 00 01  00 00 01 8C 5F 5F 54 45  ............▌__TE
00006060  58 54 00 00 00 00 00 00  00 00 00 00 00 00 10 00  XT..............
```

McAfee

Universal Binaries

- Dual Code Malware
- Intel →Jump PowerPC, placeholder, jump Intel
- Corruptions

McAfee

7- Tools

McAfee

Tools

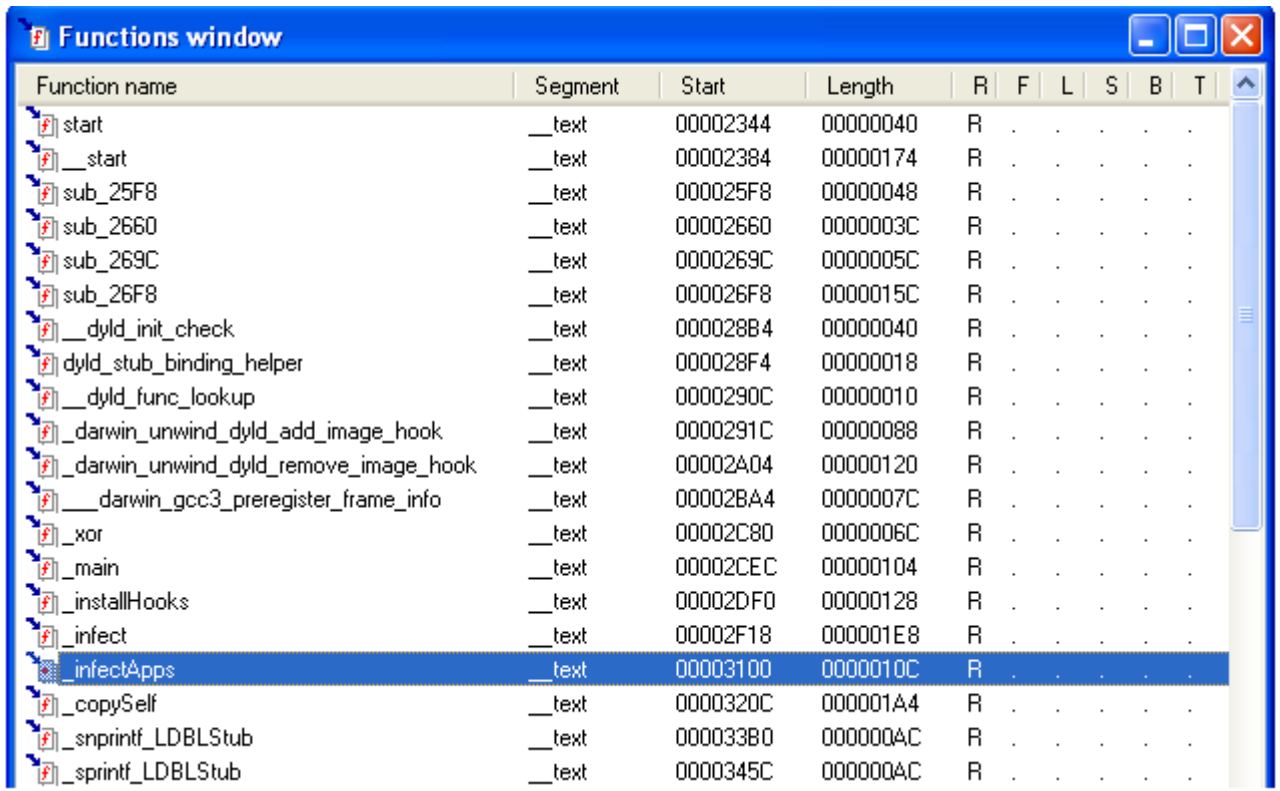
- "**otool**" - information about the file format structure
  /usr/bin/otool –hv /bin/date
- Another such tool is called "**nm**".

- For debugging **gdb** can be used.

- **dd** backup

McAfee

- **IDA** v4.9 sp1 can be usefull partially.



McAfee

8- Conclusion

McAfee

Conclusion

- OSX/Leap not perfect but proof of concept
- File-infecting viruses for the OSX platform are certainly a possibility in the near future.

McAfee

- Thanks for Attention!

  Questions?

- Marius_van_Oers@Avertlabs.com