A Deeper Look at Malware
The Whole Story

By: Bryan Lu

Virus Bulletin Conference 2007
September 19-21, 2007
Vienna, Austria

Antivirus World

Customer / Biz side

Customers meet the product
- hidden layer and a growing gap

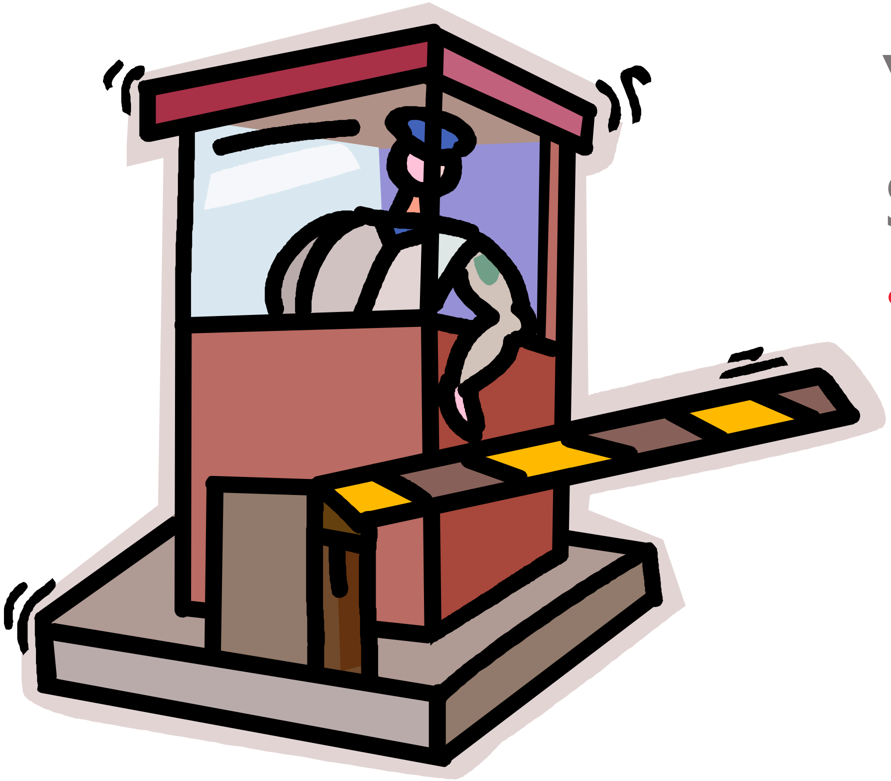
Research & Support
Teams

Disclaimer: on data, features and AV names

Agenda

- How good is the detection?
- Life span of a Malware
- The real detection rate and latest threats’ backlog
- Malware prevalence to Undetected file type
- Packed vs. Unpacked malware.
- Silver in the bags of junk
- Unused options

How good is the detection?



“Your ID please!”

Simple Enough?

- Just like scanning boot viruses (back in the days)

- Cross-detection rate based on AV-Test: 60% (lowest)?

Lifespan of a Malware

Lifespan of a Malware is the amount in time that it has existed in the wild.

Formula:

Lifespan = Last Detection Date minus Discovered Date

i.e.

On Netsky.P, May 2007 – Mar 2004 = 3 Y & 3 M

On Grew.A, May 2007 – Jan 2006 = 1 Y & 5 M

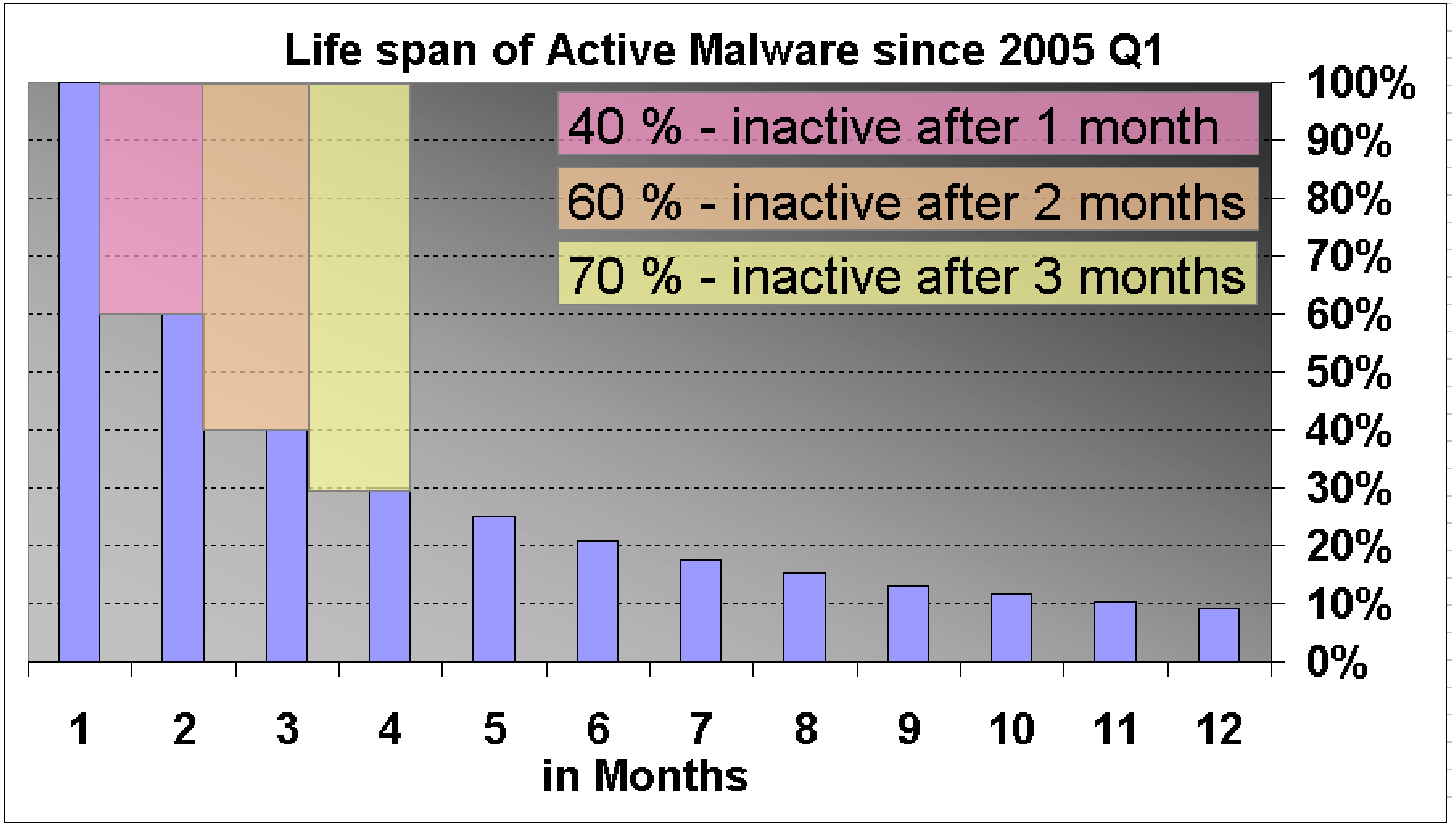
Few known limitations:

- gaps, still prevalent, by name

Lifespan of a Malware: data set

- Consists of more than 20,000 prevalent windows executable malware between January 2005 and May 2007.
- Based on several thousands of units worldwide that have been reporting their threat events.

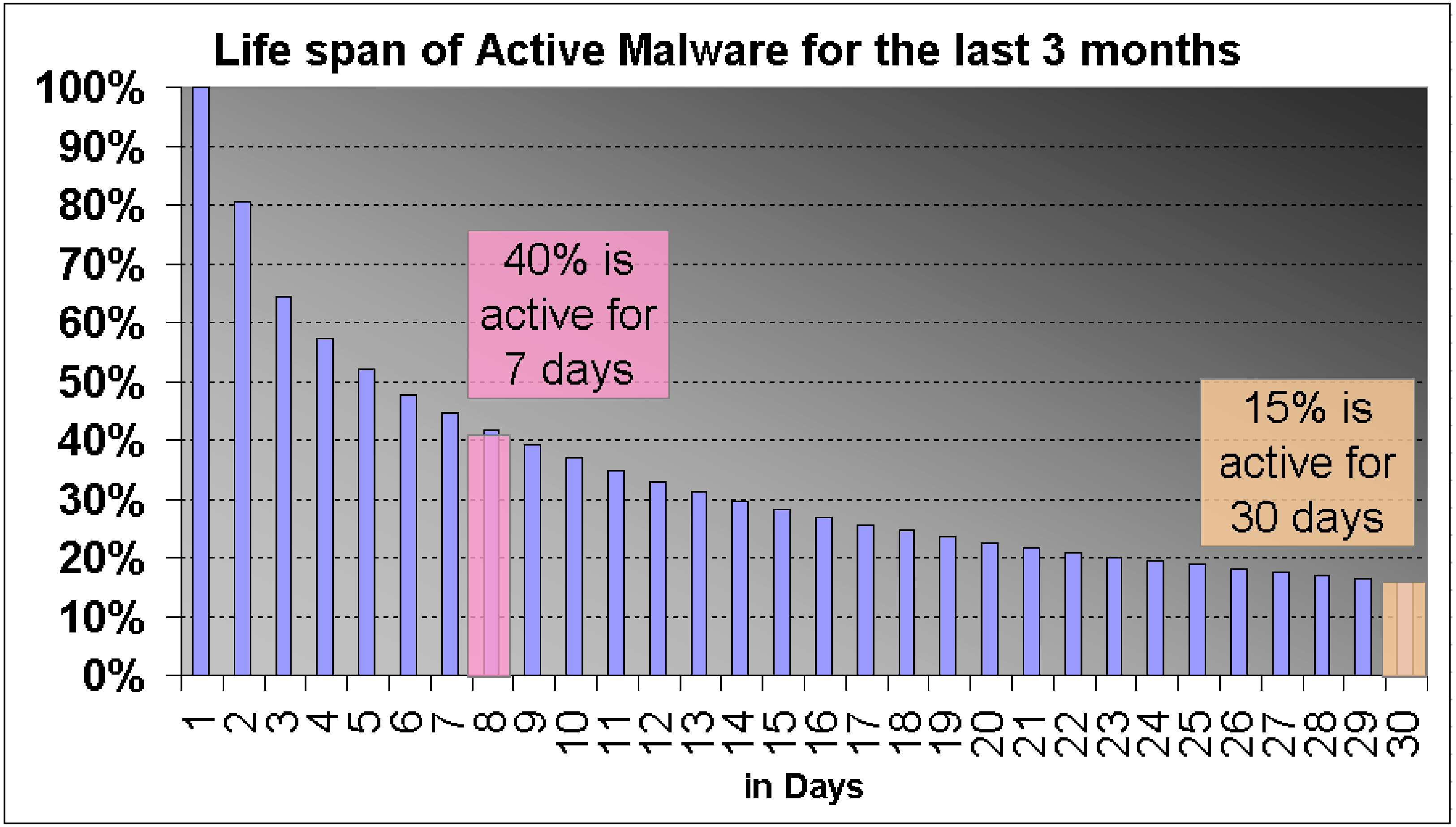
Life span of a malware: by month



- 70% of malware became inactive after 3 months

*based on Fortinet's malware Prevalence System

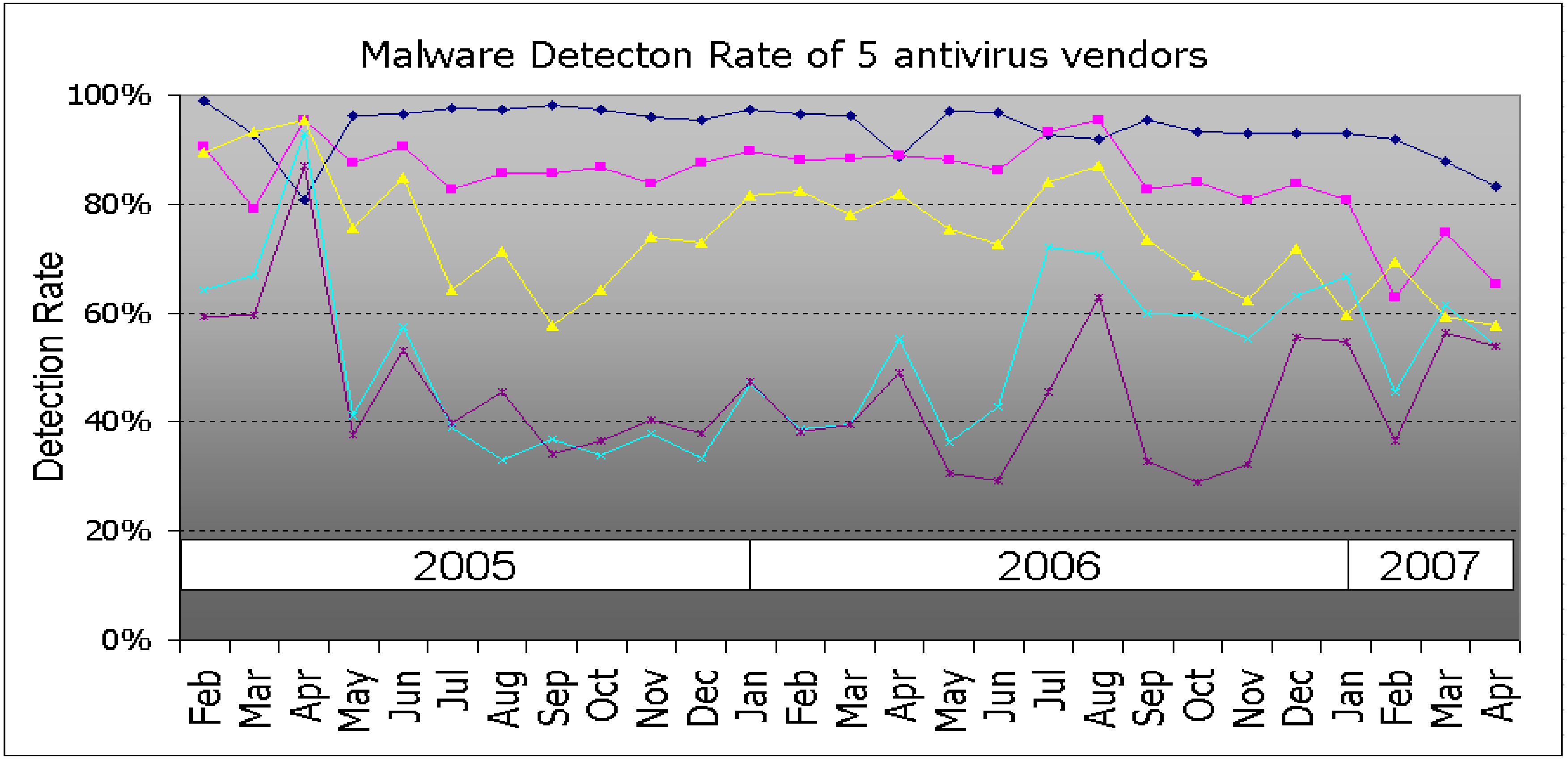
Life span of a malware: by days



- 60% of malware became inactive after 7 days.

*based on Fortinet's malware Prevalence System

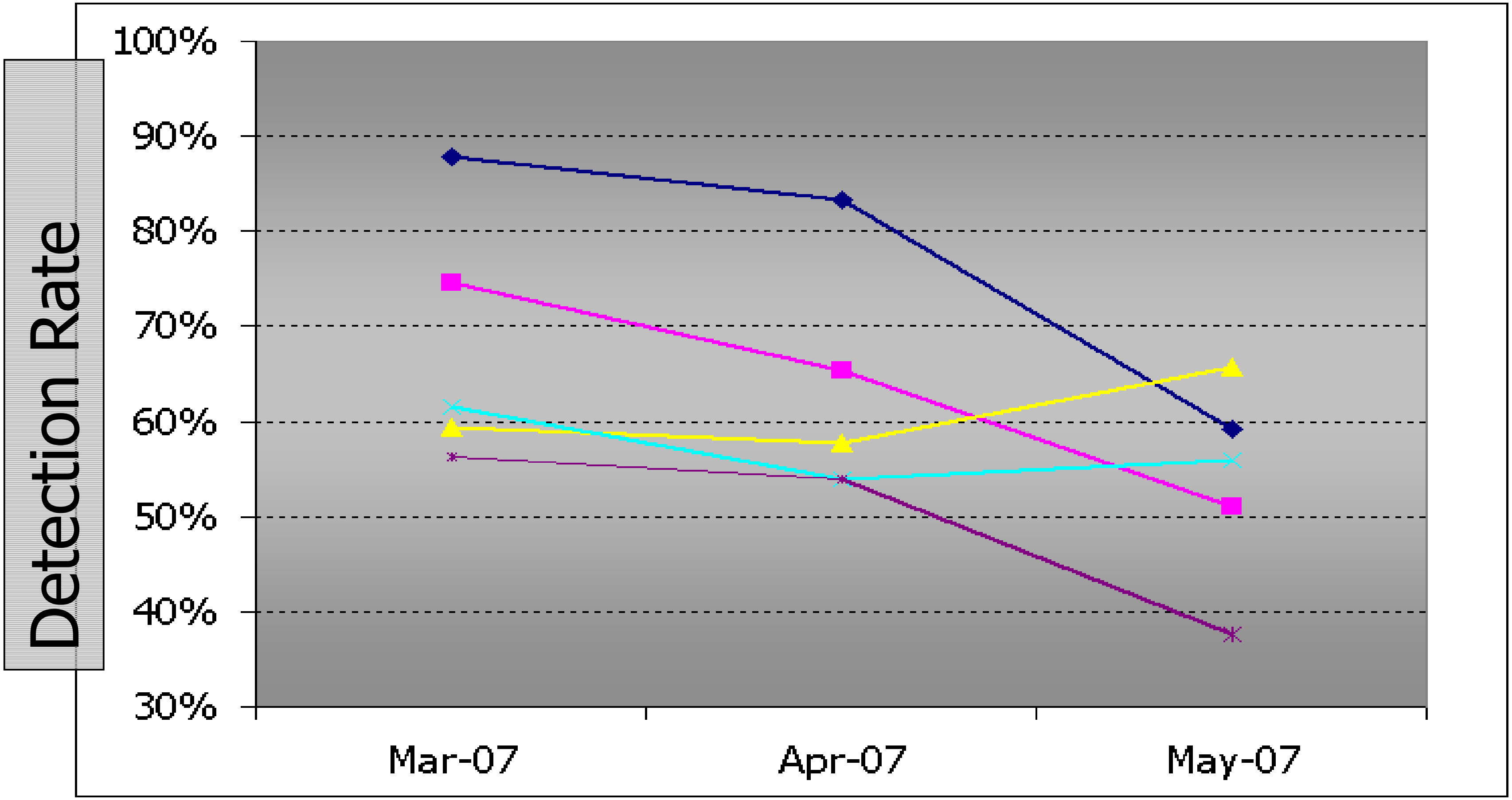
Detection Rate* (since 2005 Q1)



- by excluding the ‘rescanning’ on older than 1 month, it shows the lag in creating a signature.

*based on Fortinet’s malware collection

Latest Threats' Backlog - 3 Months



- Highest detection rate on May 2007 - **65%**

*based on Fortinet's malware collection

Malware Prevalence

- 2005
  - Windows Executable (IM-worm, Email-worm, Spyware, Trojan, Windows Virus, Network Worm, File-based exploit): 96% (580 M)
  - Scripts, Macro, Mobile, Linux, Phish:X4%
- 2006
  - Windows Executable (IM-worm, Email-worm, Spyware, Trojan, Windows Virus, Network Worm, File-based exploit): 86% (435 M)
  - Scripts, Macro, Mobile, Linux, Phish:X14%

*based on Fortinet's malware Prevalence System

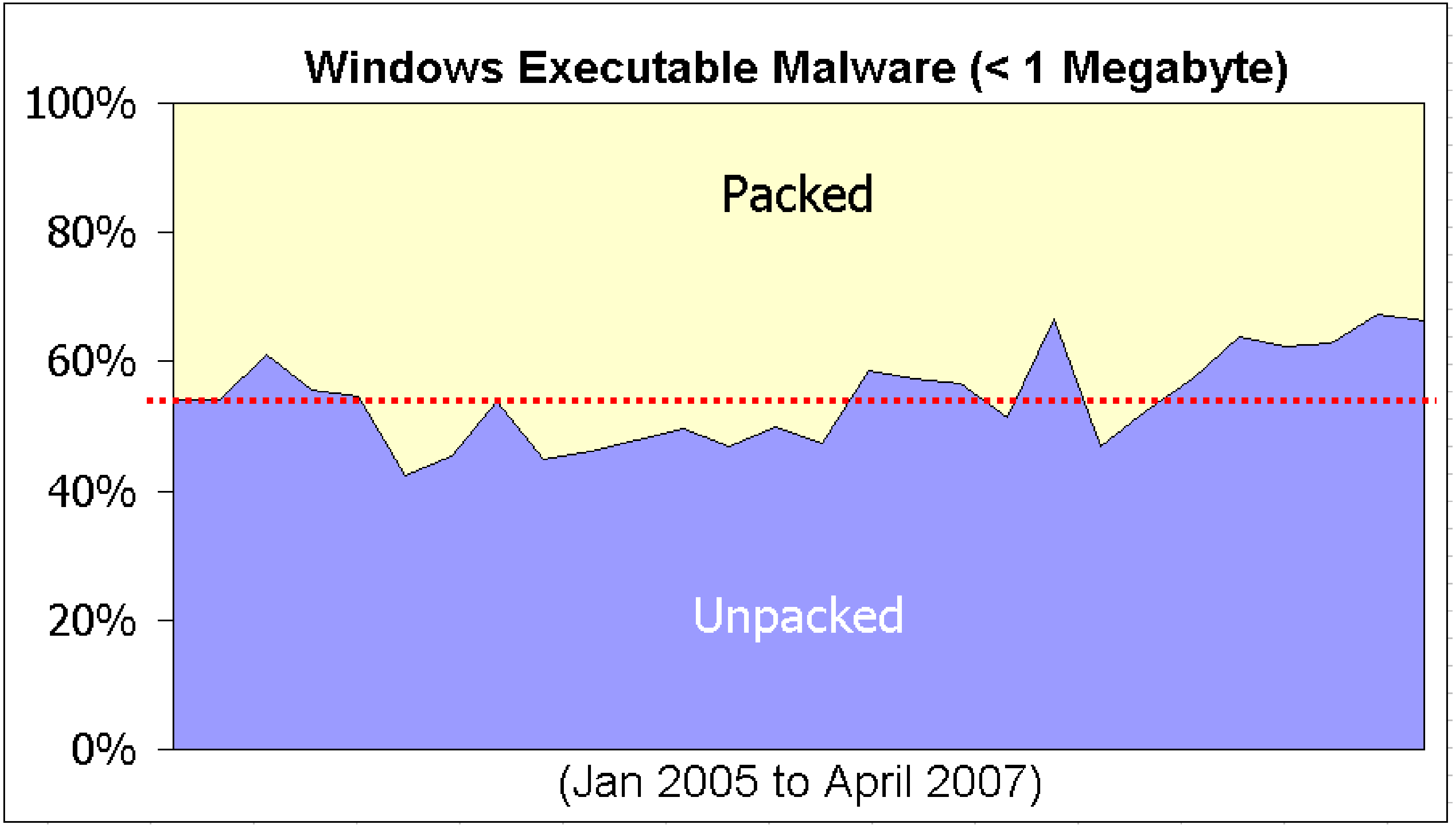
Undetected file type

Based on the top 3 scanners from the previous slide and our malware collection:

- The number of malware in windows executable format has grown (of course); however, the detection rate has not improved.
  - In 2005, 73 % is detected by the top scanners from the previous slide.
  - In 2006, 67%.
  - In 2007, **47%.**

*based on Fortinet’s malware collection

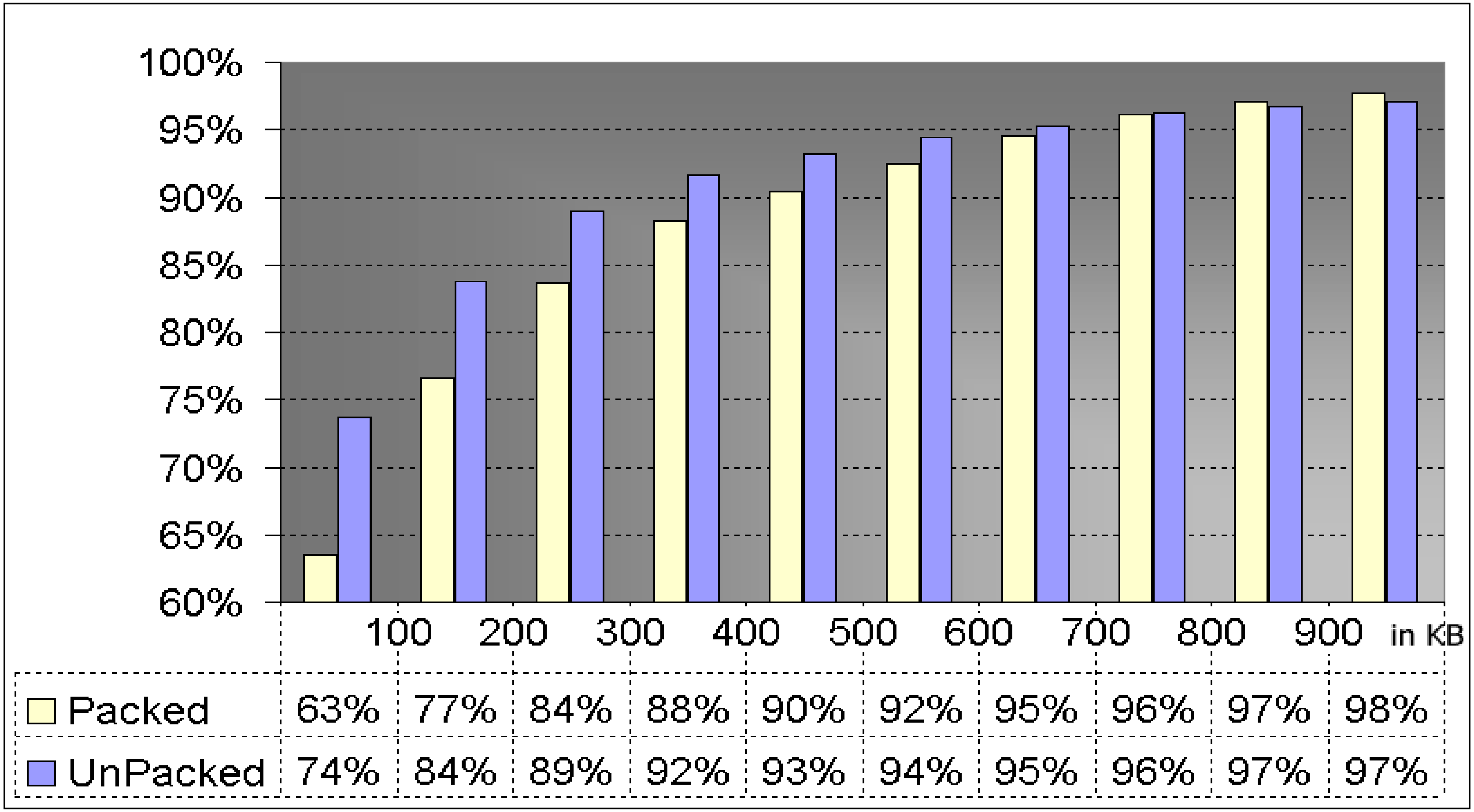
Is it Packed?



- On less than 1 MB malware, 44% are packed.

*based on Fortinet’s malware collection

And, its file sizes

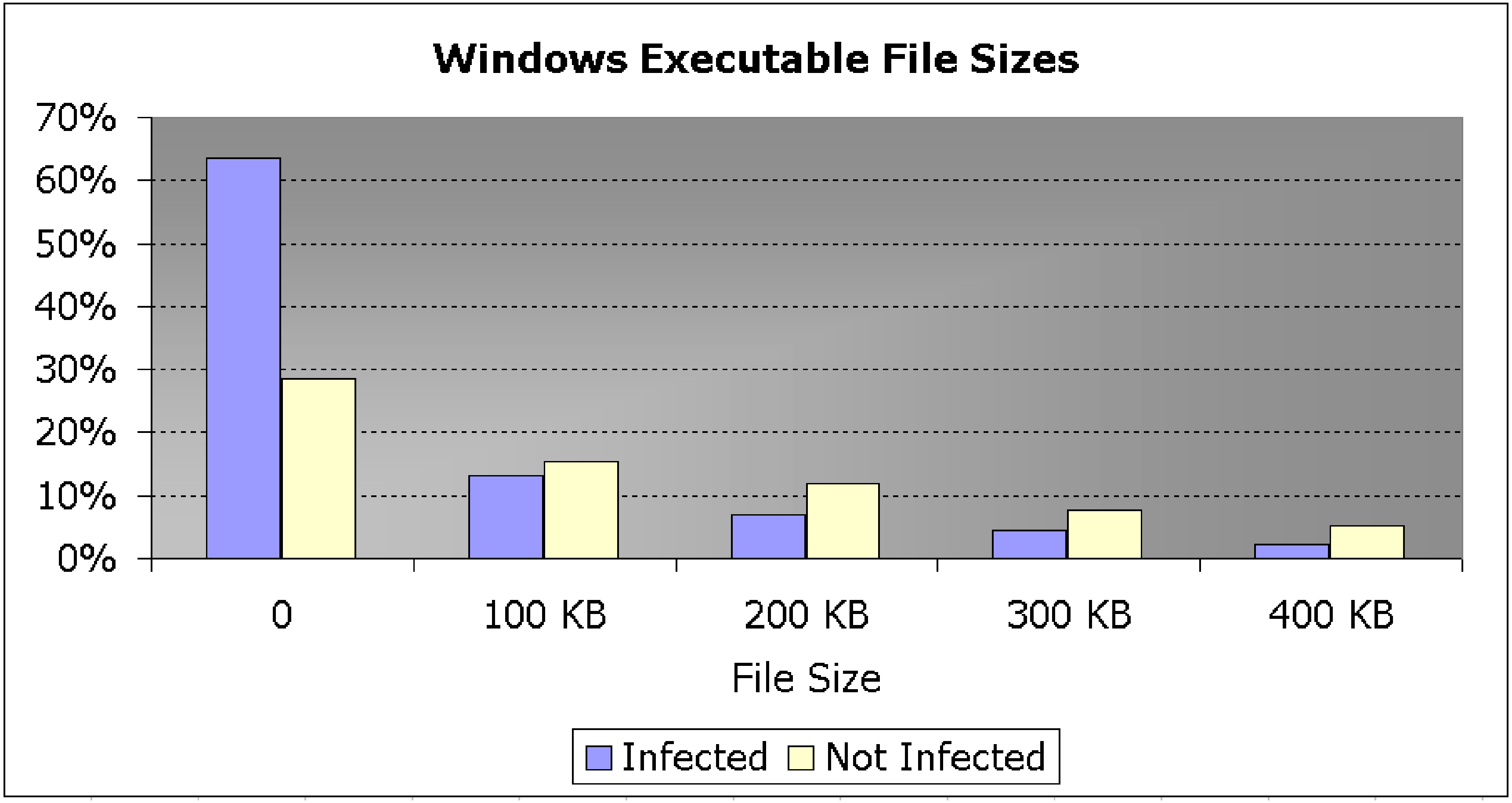


🟨 Packed	63%	77%	84%	88%	90%	92%	95%	96%	97%	98%
🟦 UnPacked	74%	84%	89%	92%	93%	94%	95%	96%	97%	97%

- 97% of packed or unpacked malware is below 1 Mbyte
- 90% of malware is below 400KB

*based on Fortinet's malware collection

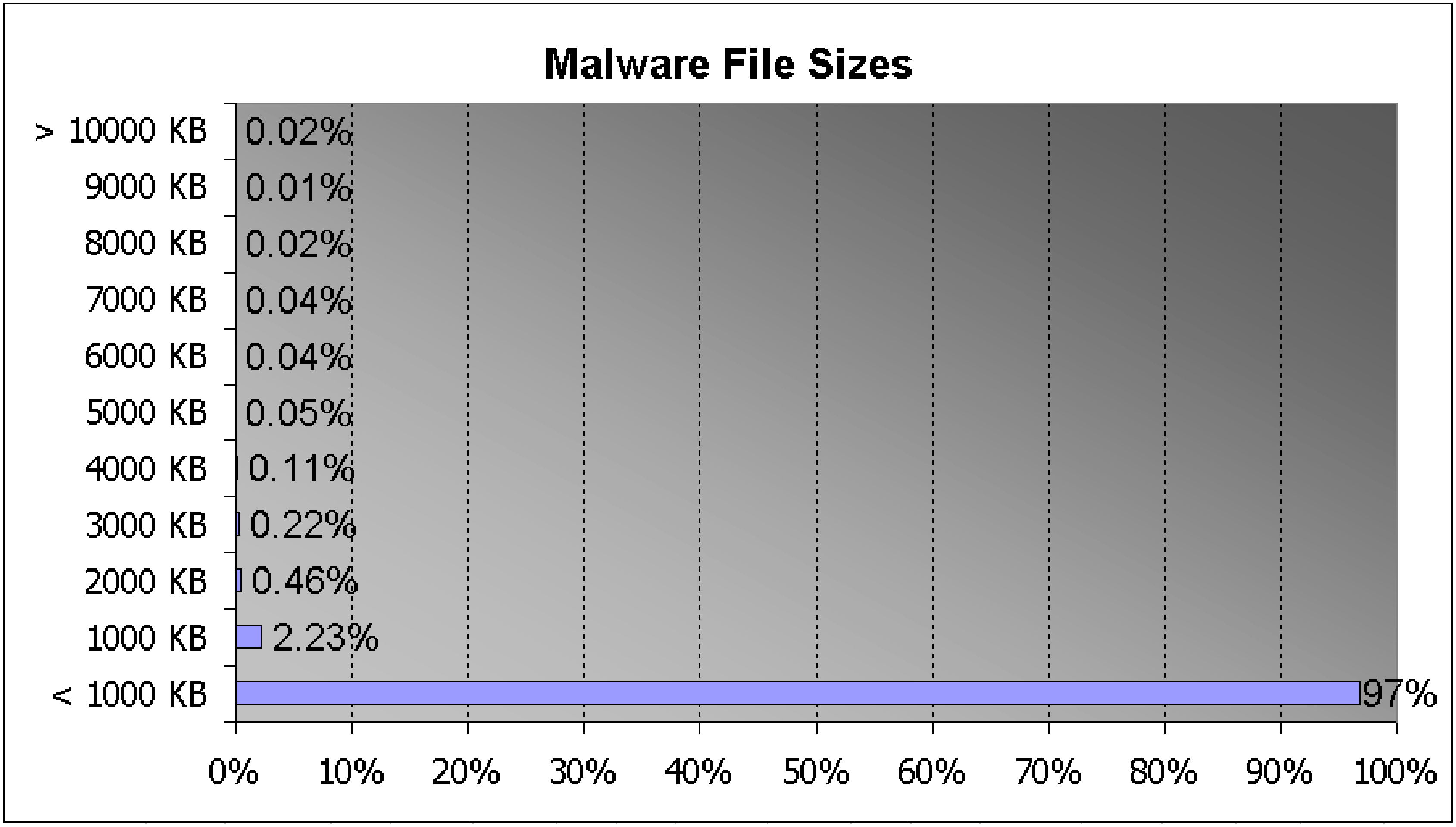
Packed Distribution



- 65% of infected malware is less than 100 KB
- 30% of normal files is less than 100 Kb

*based on Fortinet's malware collection

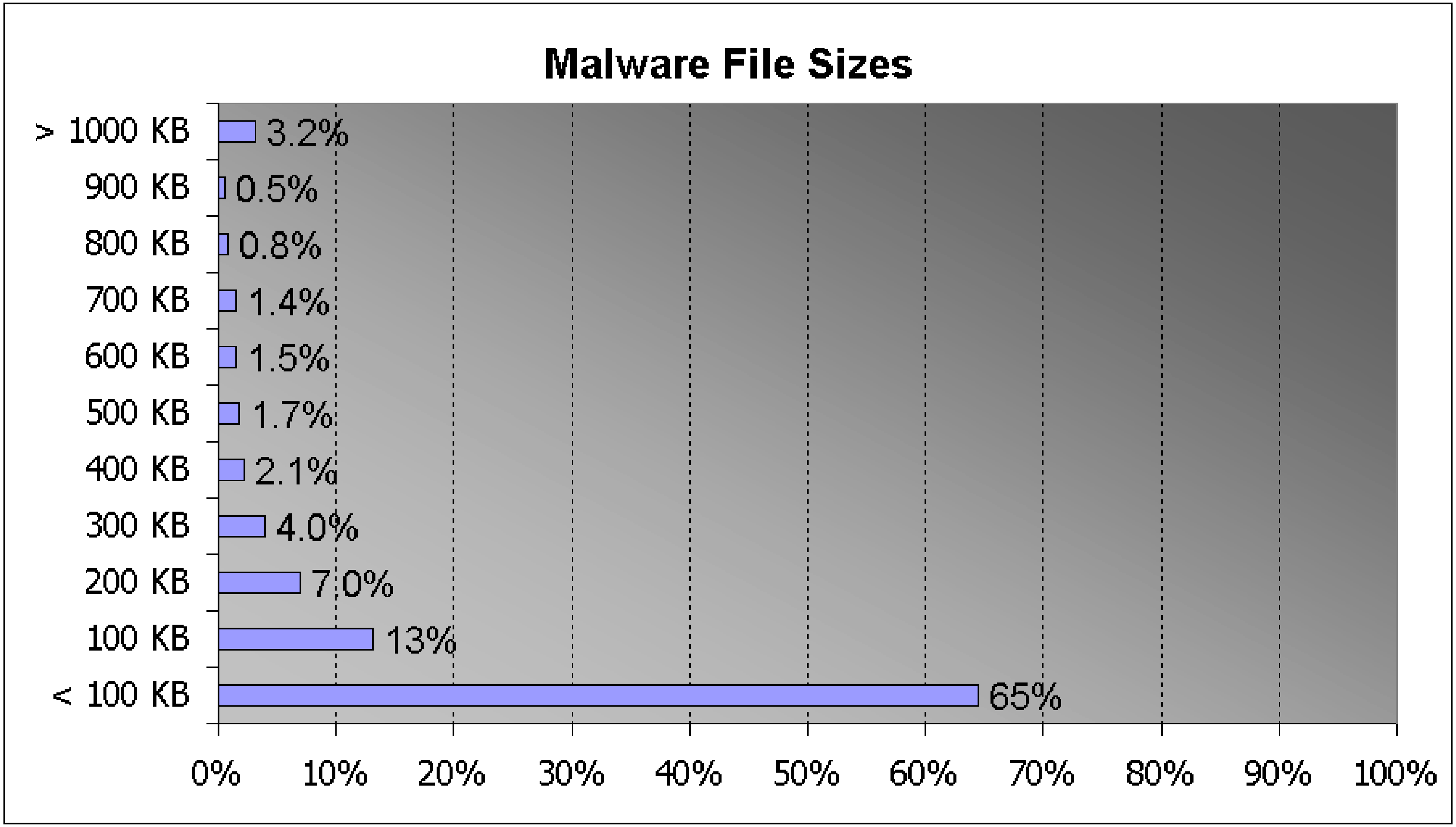
File Size limiting



- 97% of malware is less than 1,000 KB.

*based on Fortinet's malware collection

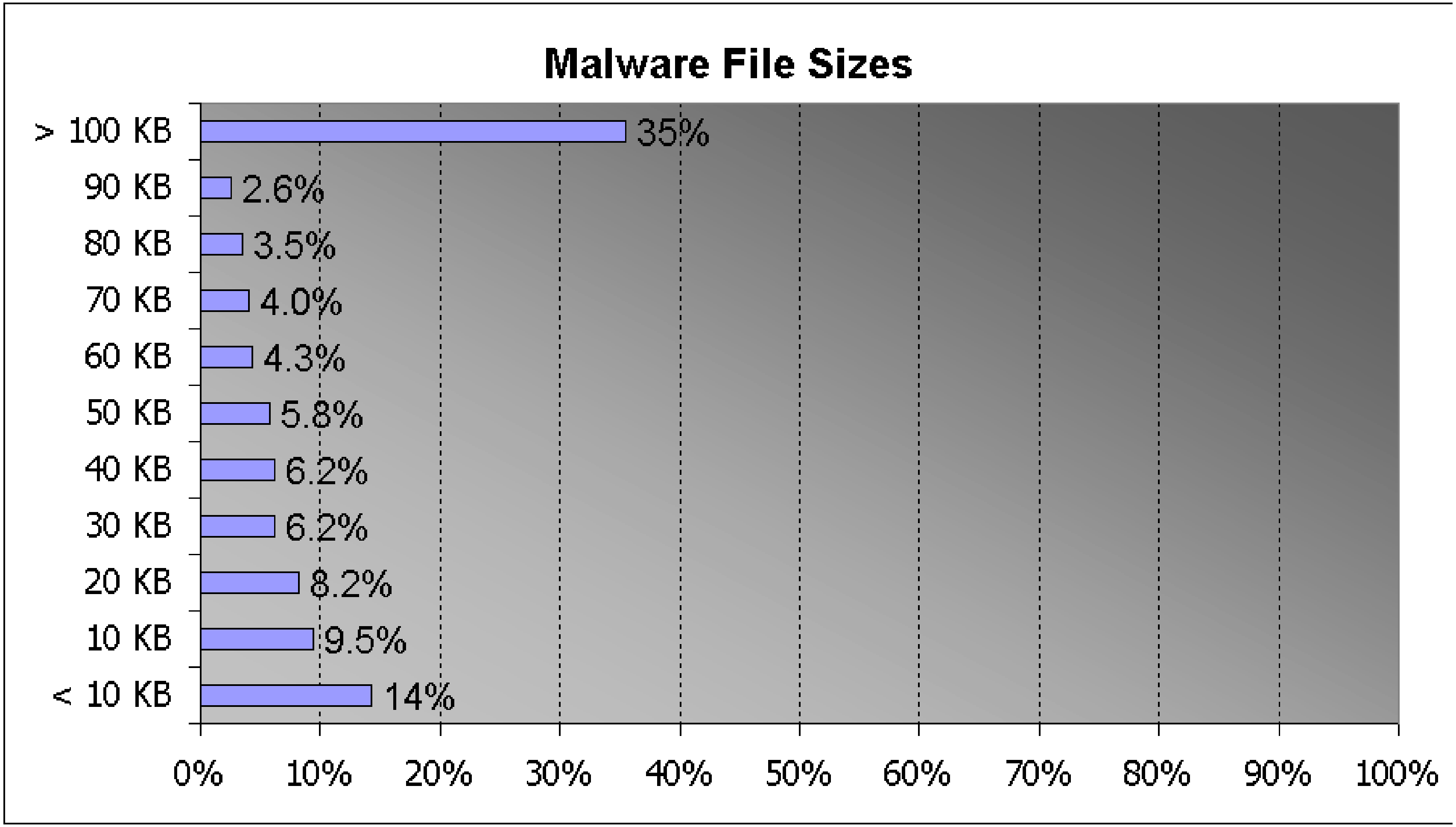
File Size limiting



- 32 % of malware is between 100 and 1000 KB

*based on Fortinet’s malware collection

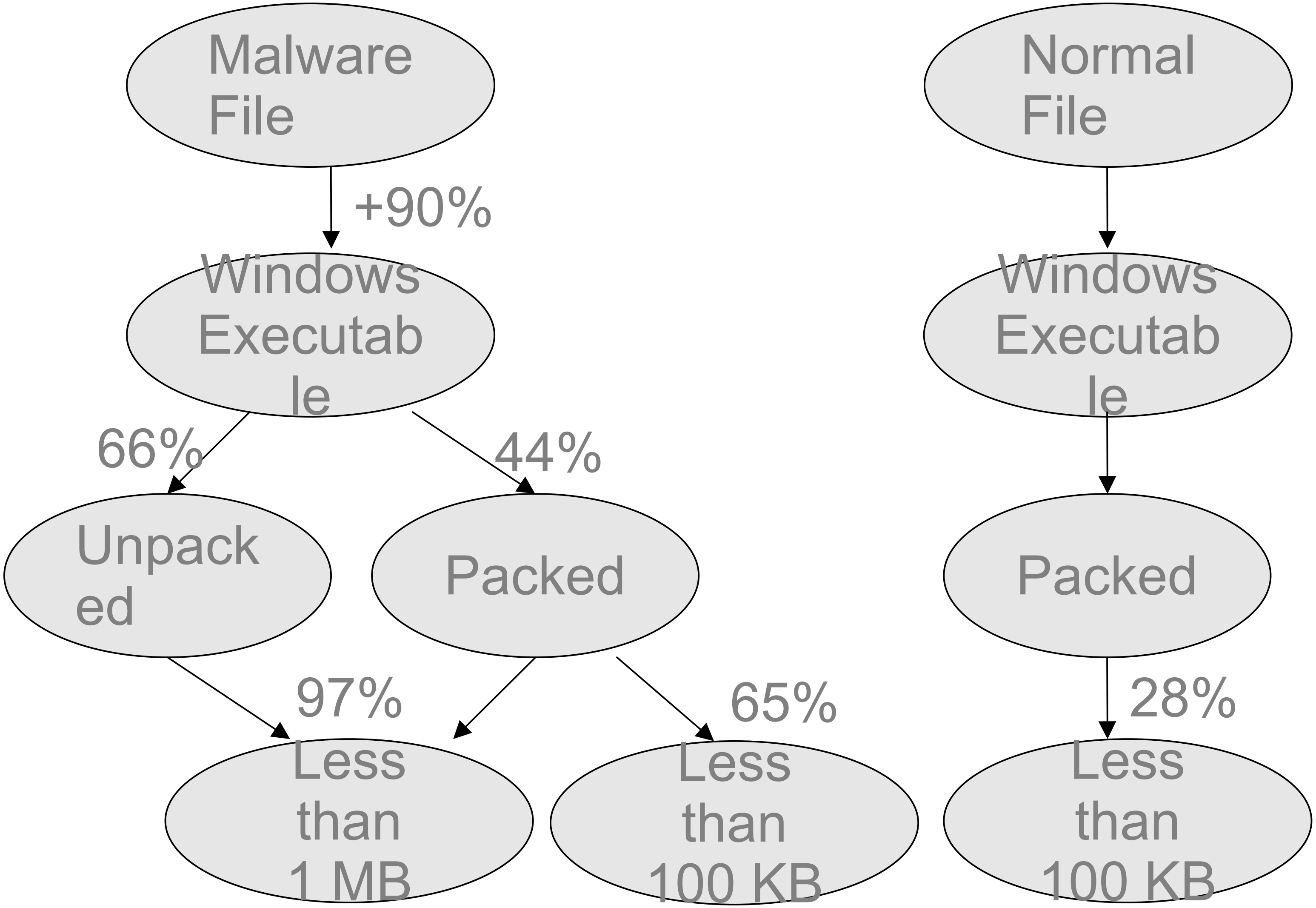
File Size limiting



- 50 percent of malware is between 10 and 100 KB

*based on Fortinet’s malware collection

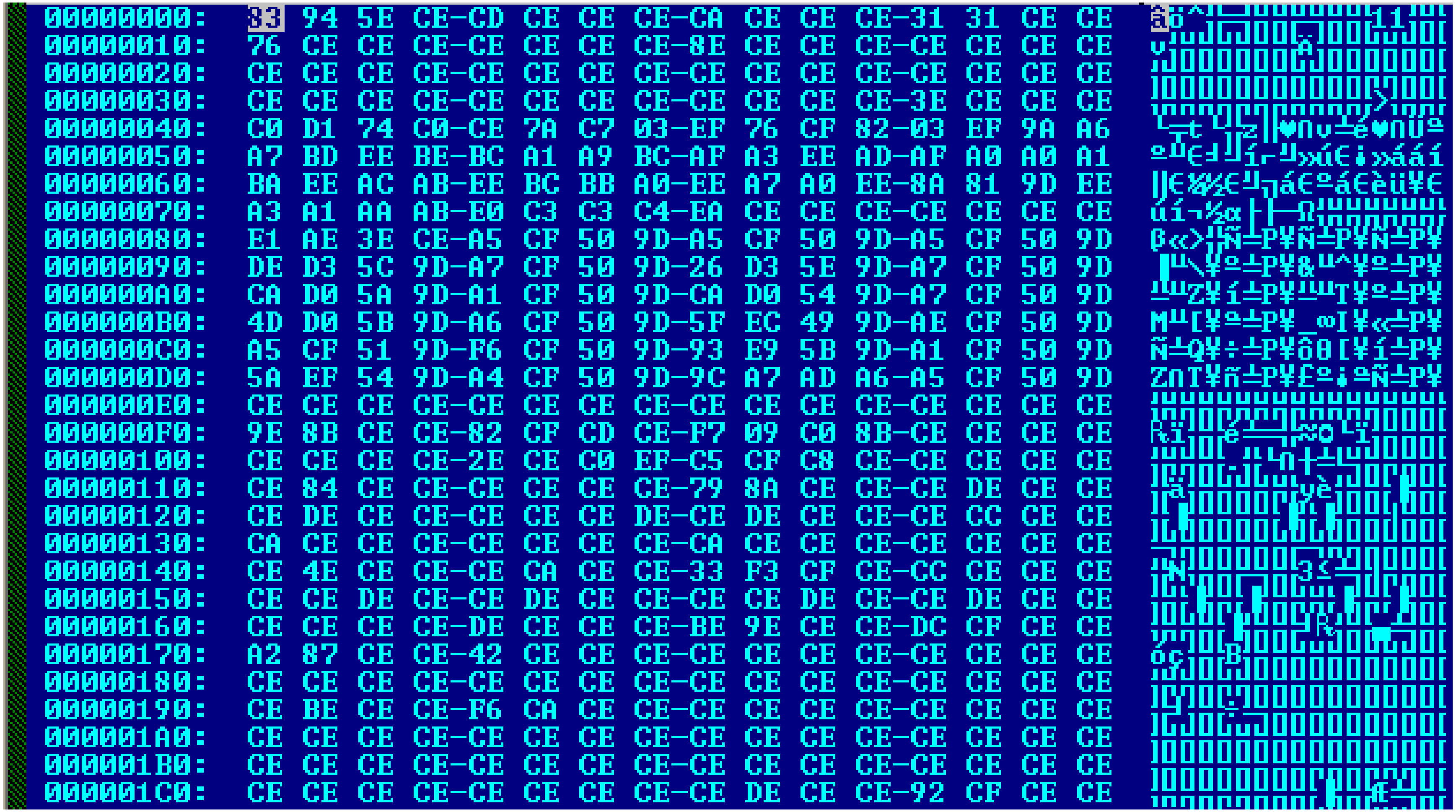
Windows Executable, Packed and Filesizes



Silver in the bags of junk

- Malware that are note-worthy because their forms are not supported
- And, they are non-executable.
- However, may be used for evading detection.

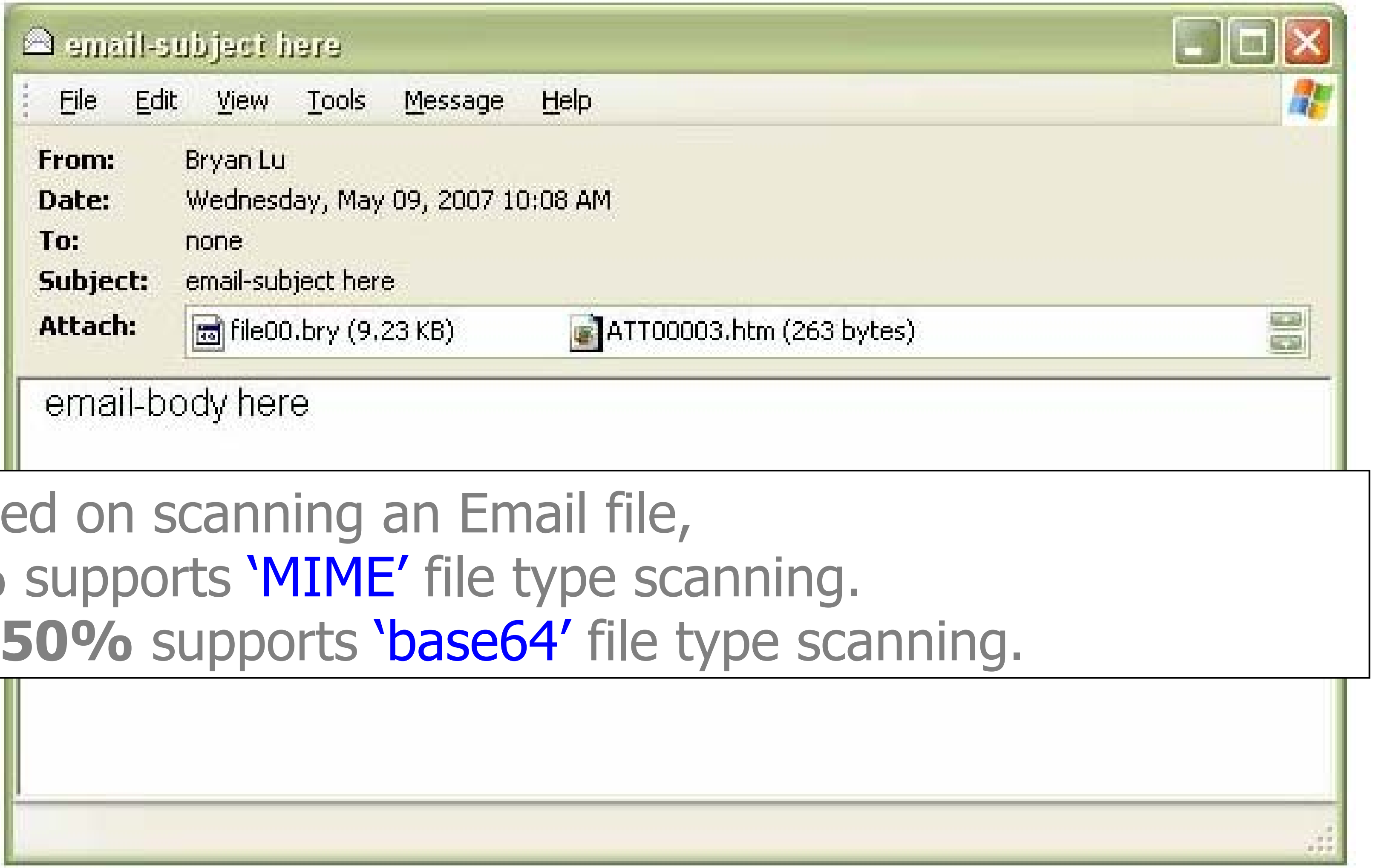
Simple Obfuscation (XOR)



```
00000000:   83 94 5E CE-CD CE CE CE-CA CE CE CE-31 31 CE CE
00000010:   76 CE CE CE-CE CE CE CE-8E CE CE CE-CE CE CE CE
00000020:   CE CE CE CE-CE CE CE CE-CE CE CE CE-CE CE CE CE
00000030:   CE CE CE CE-CE CE CE CE-CE CE CE CE-3E CE CE CE
00000040:   C0 D1 74 C0-CE 7A C7 03-EF 76 CF 82-03 EF 9A A6
00000050:   A7 BD EE BE-BC A1 A9 BC-AF A3 EE AD-AF A0 A0 A1
00000060:   BA EE AC AB-EE BC BB A0-EE A7 A0 EE-8A 81 9D EE
00000070:   A3 A1 AA AB-E0 C3 C3 C4-EA CE CE CE-CE CE CE CE
00000080:   E1 AE 3E CE-A5 CF 50 9D-A5 CF 50 9D-A5 CF 50 9D
00000090:   DE D3 5C 9D-A7 CF 50 9D-26 D3 5E 9D-A7 CF 50 9D
000000A0:   CA D0 5A 9D-A1 CF 50 9D-CA D0 54 9D-A7 CF 50 9D
000000B0:   4D D0 5B 9D-A6 CF 50 9D-5F EC 49 9D-AE CF 50 9D
000000C0:   A5 CF 51 9D-F6 CF 50 9D-93 E9 5B 9D-A1 CF 50 9D
000000D0:   5A EF 54 9D-A4 CF 50 9D-9C A7 AD A6-A5 CF 50 9D
000000E0:   CE CE CE CE-CE CE CE CE-CE CE CE CE-CE CE CE CE
000000F0:   9E 8B CE CE-82 CF CD CE-F7 09 C0 8B-CE CE CE CE
00000100:   CE CE CE CE-2E CE C0 EF-C5 CF C8 CE-CE CE CE CE
00000110:   CE 84 CE CE-CE CE CE CE-79 8A CE CE-CE DE CE CE
00000120:   CE DE CE CE-CE CE CE DE-CE DE CE CE-CE CC CE CE
00000130:   CA CE CE CE-CE CE CE CE-CA CE CE CE-CE CE CE CE
00000140:   CE 4E CE CE-CE CA CE CE-33 F3 CF CE-CC CE CE CE
00000150:   CE CE DE CE-CE DE CE CE-CE CE DE CE-CE DE CE CE
00000160:   CE CE CE CE-DE CE CE CE-BE 9E CE CE-DC CF CE CE
00000170:   A2 87 CE CE-42 CE CE CE-CE CE CE CE-CE CE CE CE
00000180:   CE CE CE CE-CE CE CE CE-CE CE CE CE-CE CE CE CE
00000190:   CE BE CE CE-F6 CA CE CE-CE CE CE CE-CE CE CE CE
000001A0:   CE CE CE CE-CE CE CE CE-CE CE CE CE-CE CE CE CE
000001B0:   CE CE CE CE-CE CE CE CE-CE CE CE CE-CE CE CE CE
000001C0:   CE CE CE CE-CE CE CE CE-CE DE CE CE-92 CF CE CE
```

- Less than 40% supports XOR

E-Mail file type



From: Bryan Lu

Date: Wednesday, May 09, 2007 10:08 AM

To: none

Subject: email-subject here

Attach: file00.bry (9.23 KB) ATT00003.htm (263 bytes)

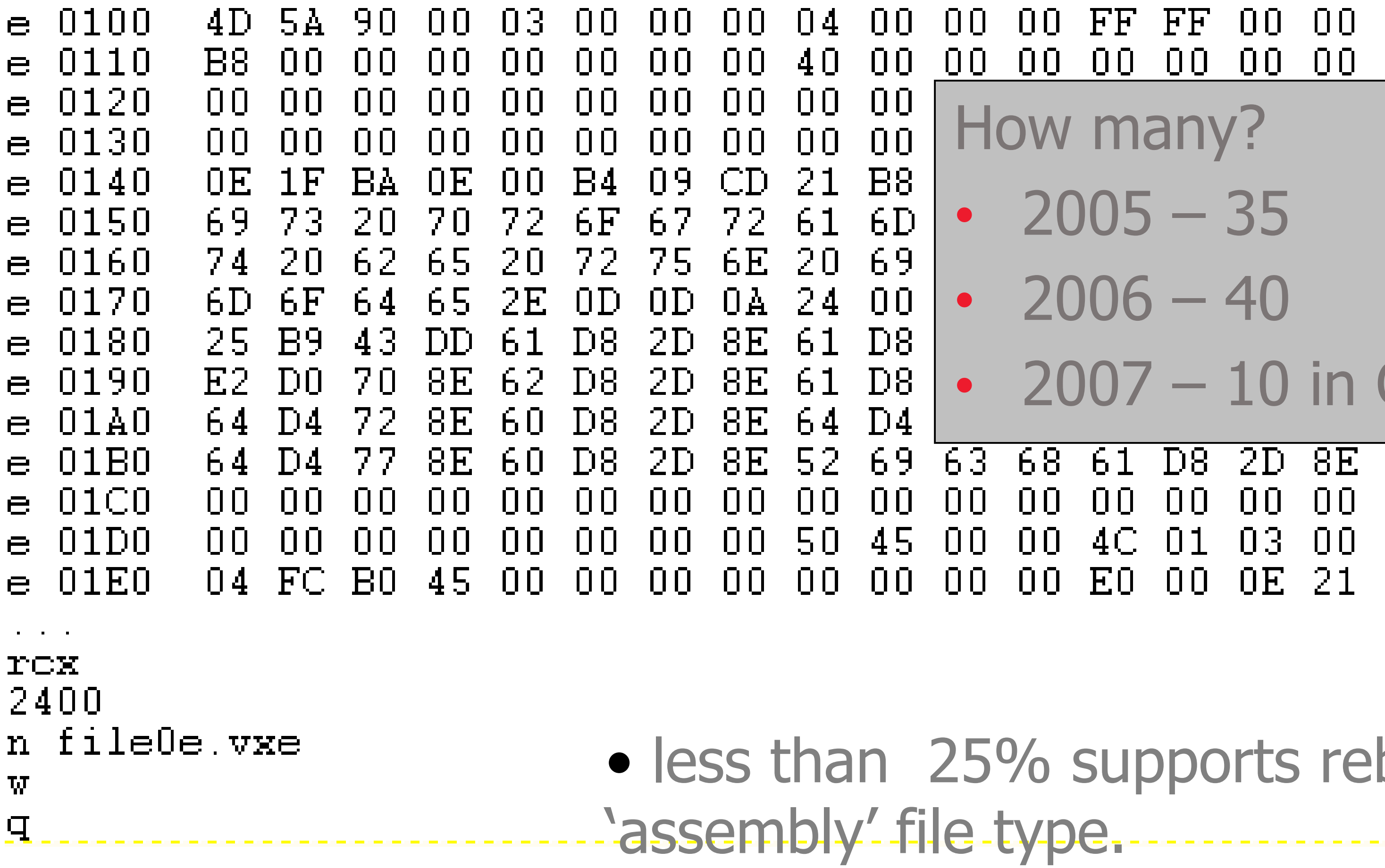
email-body here

- Based on scanning an Email file,

70% supports ‘MIME’ file type scanning.

And, **50%** supports ‘base64’ file type scanning.

Assembly file type



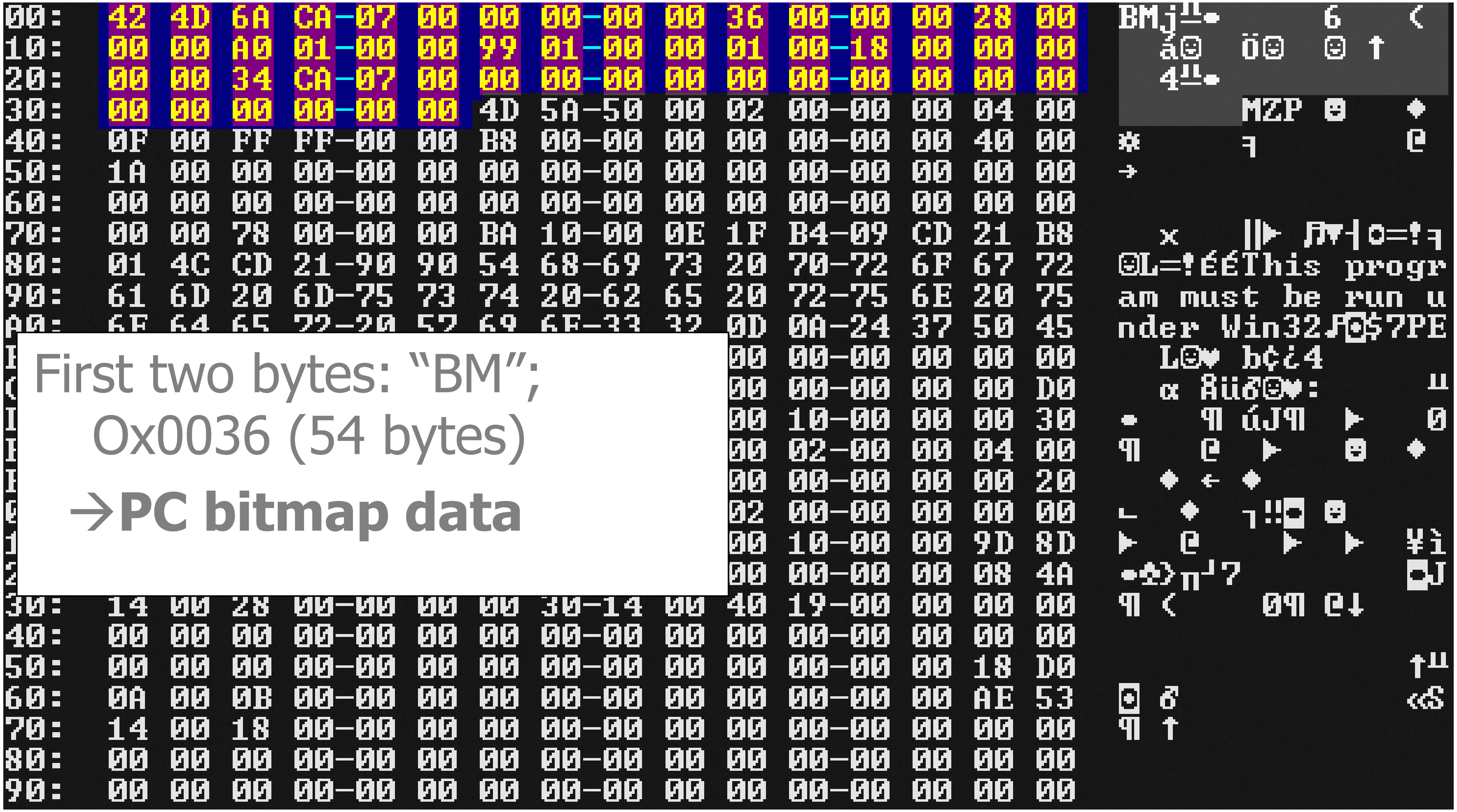
```
e 0100  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
e 0110  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
e 0120  00 00 00 00 00 00 00 00 00 00
e 0130  00 00 00 00 00 00 00 00 00 00
e 0140  0E 1F BA 0E 00 B4 09 CD 21 B8
e 0150  69 73 20 70 72 6F 67 72 61 6D
e 0160  74 20 62 65 20 72 75 6E 20 69
e 0170  6D 6F 64 65 2E 0D 0D 0A 24 00
e 0180  25 B9 43 DD 61 D8 2D 8E 61 D8
e 0190  E2 D0 70 8E 62 D8 2D 8E 61 D8
e 01A0  64 D4 72 8E 60 D8 2D 8E 64 D4
e 01B0  64 D4 77 8E 60 D8 2D 8E 52 69 63 68 61 D8 2D 8E
e 01C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
e 01D0  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 03 00
e 01E0  04 FC B0 45 00 00 00 00 00 00 00 00 E0 00 0E 21
...
rcx
2400
n file0e.vxe
w
q
```

How many?

- 2005 – 35
- 2006 – 40
- 2007 – 10 in Q1

- less than 25% supports rebuilding 'assembly' file type.

BMP + EXE Header



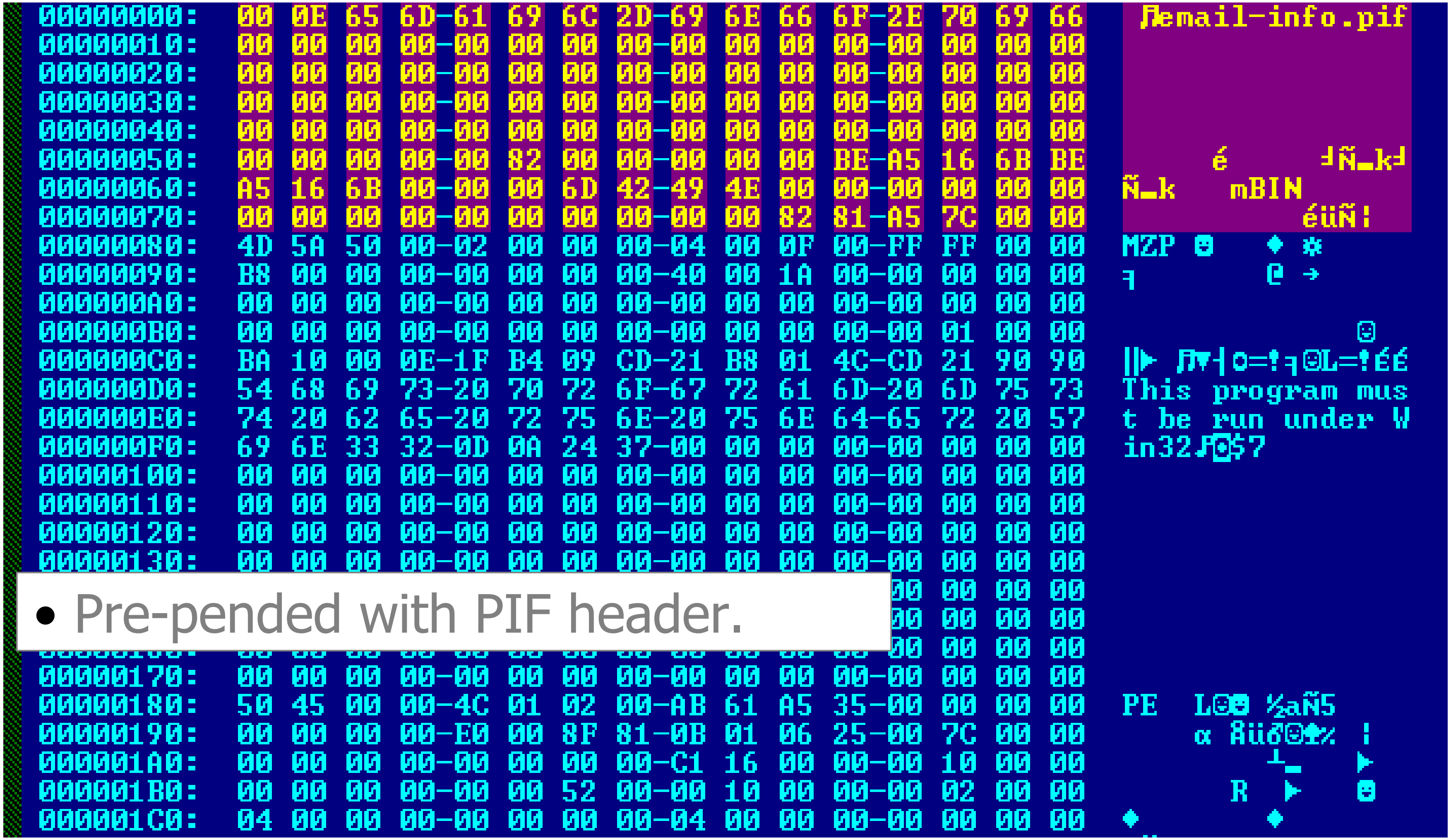
```
00:  42 4D 6A CA-07 00 00 00-00 00 36 00-00 00 28 00   BMj╩•     6   (
10:  00 00 A0 01-00 00 99 01-00 00 01 00-18 00 00 00     á☺  Ö☺  ☺ ↑
20:  00 00 34 CA-07 00 00 00-00 00 00 00-00 00 00 00     4╩•
30:  00 00 00 00-00 00 4D 5A-50 00 02 00-00 00 04 00         MZP ☻  ♦
40:  0F 00 FF FF-00 00 B8 00-00 00 00 00-00 00 40 00   ☼     ╕      @
50:  1A 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00   →
60:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
70:  00 00 78 00-00 00 BA 10-00 0E 1F B4-09 CD 21 B8     x   ║►  ♫▼┤○═!╕
80:  01 4C CD 21-90 90 54 68-69 73 20 70-72 6F 67 72   ☺L═!ÉÉThis progr
90:  61 6D 20 6D-75 73 74 20-62 65 20 72-75 6E 20 75   am must be run u
A0:  6E 64 65 72-20 57 69 6E-33 32 0D 0A-24 37 50 45   nder Win32♪◙$7PE
                                      00 00-00 00 00 00      L☺♥ b¢¿4
                                      00 00-00 00 00 D0      α ÅüΘ☺♥:     ╨
                                      00 10-00 00 00 30    •    ¶ úJ¶  ►   0
                                      00 02-00 00 04 00    ¶   @   ►   ☻   ♦
                                      00 00-00 00 00 20       ♦ ← ♦
                                      02 00-00 00 00 00    └   ♦  ┐‼☻ ☻
                                      00 10-00 00 9D 8D    ►  @     ►  ►  ¥ì
                                      00 00-00 00 08 4A    •♫}π┘7         ◘J
30:  14 00 28 00-00 00 00 30-14 00 40 19-00 00 00 00   ¶ (    0¶ @↓
40:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
50:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 18 D0                 ↑╨
60:  0A 00 0B 00-00 00 00 00-00 00 00 00-00 00 AE 53   ◙ ♂            «S
70:  14 00 18 00-00 00 00 00-00 00 00 00-00 00 00 00   ¶ ↑
80:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
90:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
```

First two bytes: “BM”;
Ox0036 (54 bytes)

→**PC bitmap data**

- less than 25% supports pre-pended bitmap header.

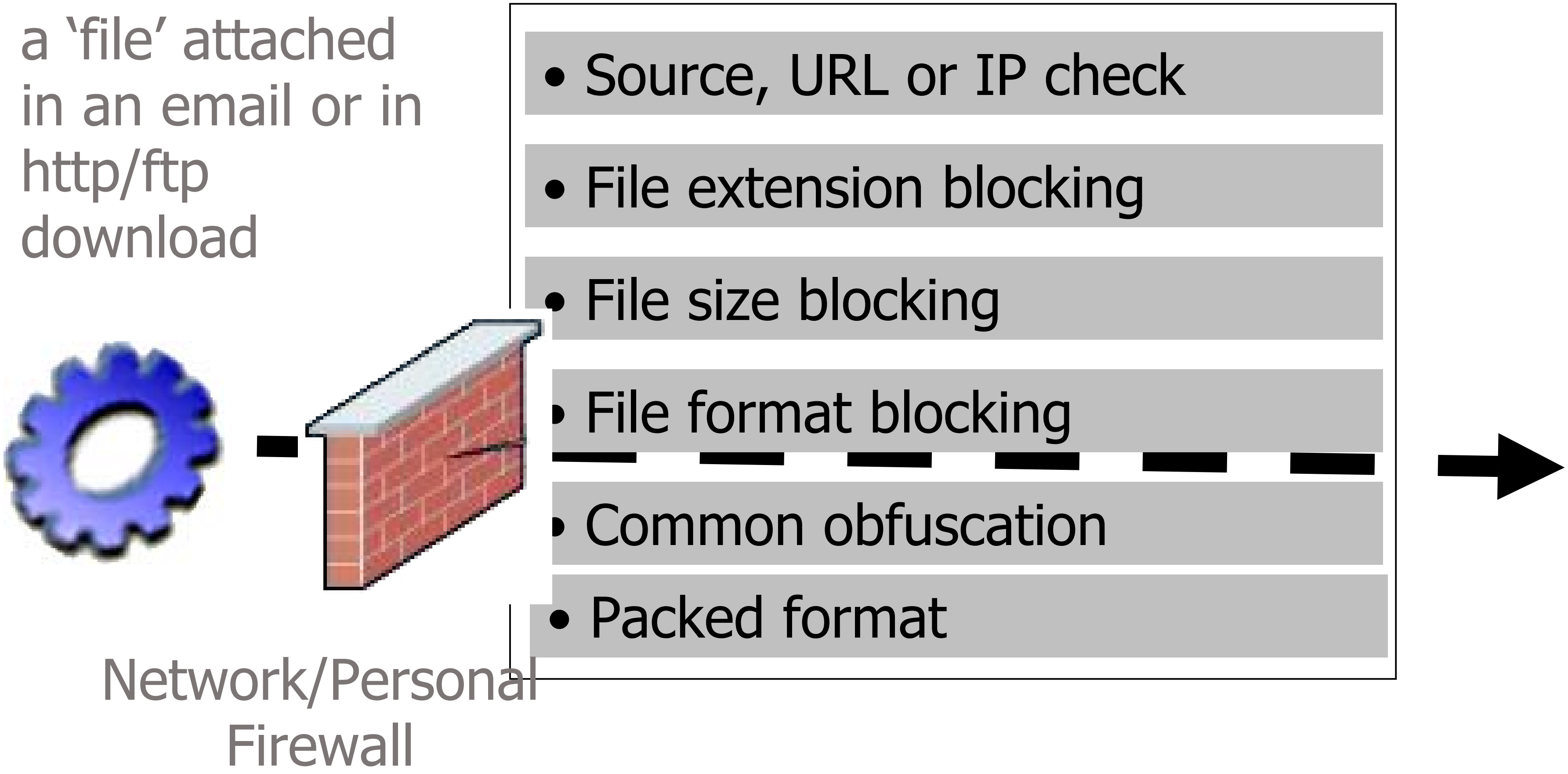
PIF/Mac Binary + EXE Header



```
00000000:  00 0E 65 6D-61 69 6C 2D-69 6E 66 6F-2E 70 69 66   ♫email-info.pif
00000010:  00 00 00 00-00 00 00 00-00 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 00-00 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 82 00 00-00 00 00 BE-A5 16 6B BE        é     ╛Ñ▬k╛
00000060:  A5 16 6B 00-00 00 6D 42-49 4E 00 00-00 00 00 00  Ñ▬k   mBIN
00000070:  00 00 00 00-00 00 00 00-00 00 82 81-A5 7C 00 00            éüÑ|
00000080:  4D 5A 50 00-02 00 00 00-04 00 0F 00-FF FF 00 00  MZP ☻   ♦ ☼
00000090:  B8 00 00 00-00 00 00 00-40 00 1A 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 00-01 00 00 00              ☺
000000C0:  BA 10 00 0E-1F B4 09 CD-21 B8 01 4C-CD 21 90 90  ║► ♫▼┤○═!╕☺L═!ÉÉ
000000D0:  54 68 69 73-20 70 72 6F-67 72 61 6D-20 6D 75 73  This program mus
000000E0:  74 20 62 65-20 72 75 6E-20 75 6E 64-65 72 20 57  t be run under W
000000F0:  69 6E 33 32-0D 0A 24 37-00 00 00 00-00 00 00 00  in32♪◙$7
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:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
                                               00 00 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:  50 45 00 00-4C 01 02 00-AB 61 A5 35-00 00 00 00  PE  L☺☻ ½aÑ5
00000190:  00 00 00 00-E0 00 8F 81-0B 01 06 25-00 7C 00 00      α Åü♂☺♠% |
000001A0:  00 00 00 00-00 00 00 00-C1 16 00 00-00 10 00 00          ┴▬   ►
000001B0:  00 00 00 00-00 52 00 00-10 00 00 00-02 00 00 00       R  ►   ☻
000001C0:  04 00 00 00-00 00 00 00-04 00 00 00-00 00 00 00  ♦       ♦
```

- Pre-pended with PIF header.

Unused Options?

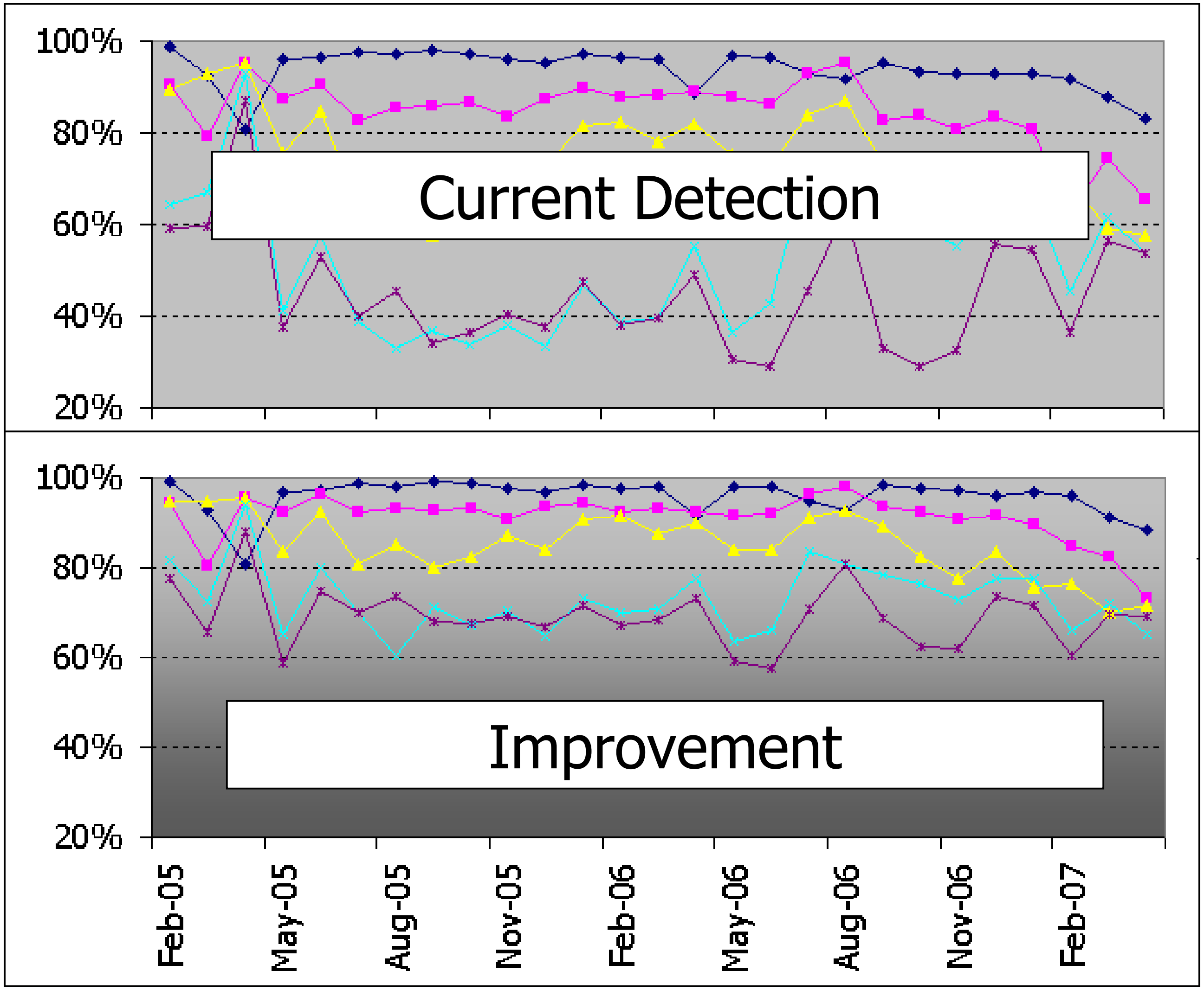


a 'file' attached in an email or in http/ftp download

- Source, URL or IP check
- File extension blocking
- File size blocking
- File format blocking
- Common obfuscation
- Packed format

Network/Personal Firewall

Blocking packed executable files



Average Improvement:

1ST Line: 6%;

2nd Line: 8%

3rd Line: 16%

4th Line: 48%

5th Line: 60%

Summary

- Analysis, Detection, Analysis, Detection ...
- 1-month Life span
  - 30% Active in the last 2 years
  - 15% Active in the last 6 months
- Advance our products with features that are based on statistical analysis.
  - Windows Executable, Packed, junk malware, file sizes, file format,

Thank you.

Q & A

bryanlu@fortinet.com

FORTINET