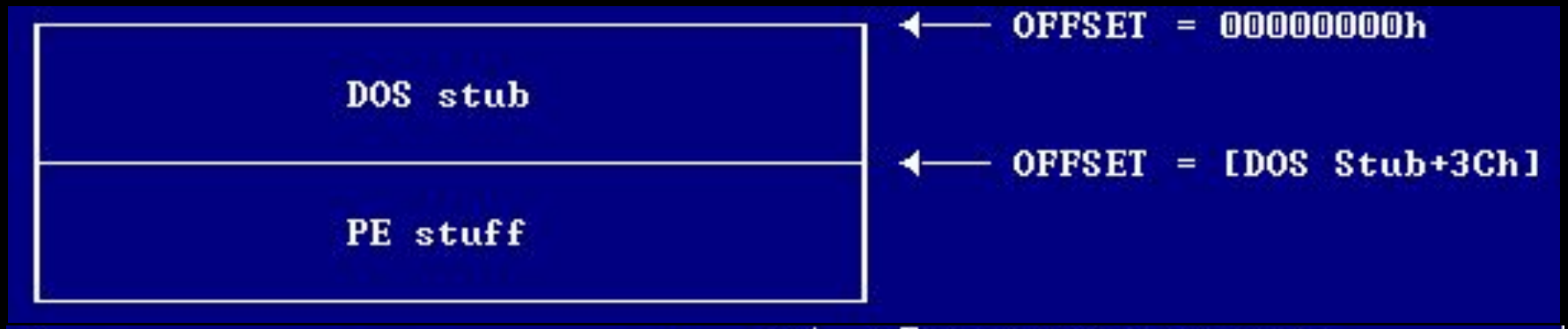
Вирусы для файлов в формате PE

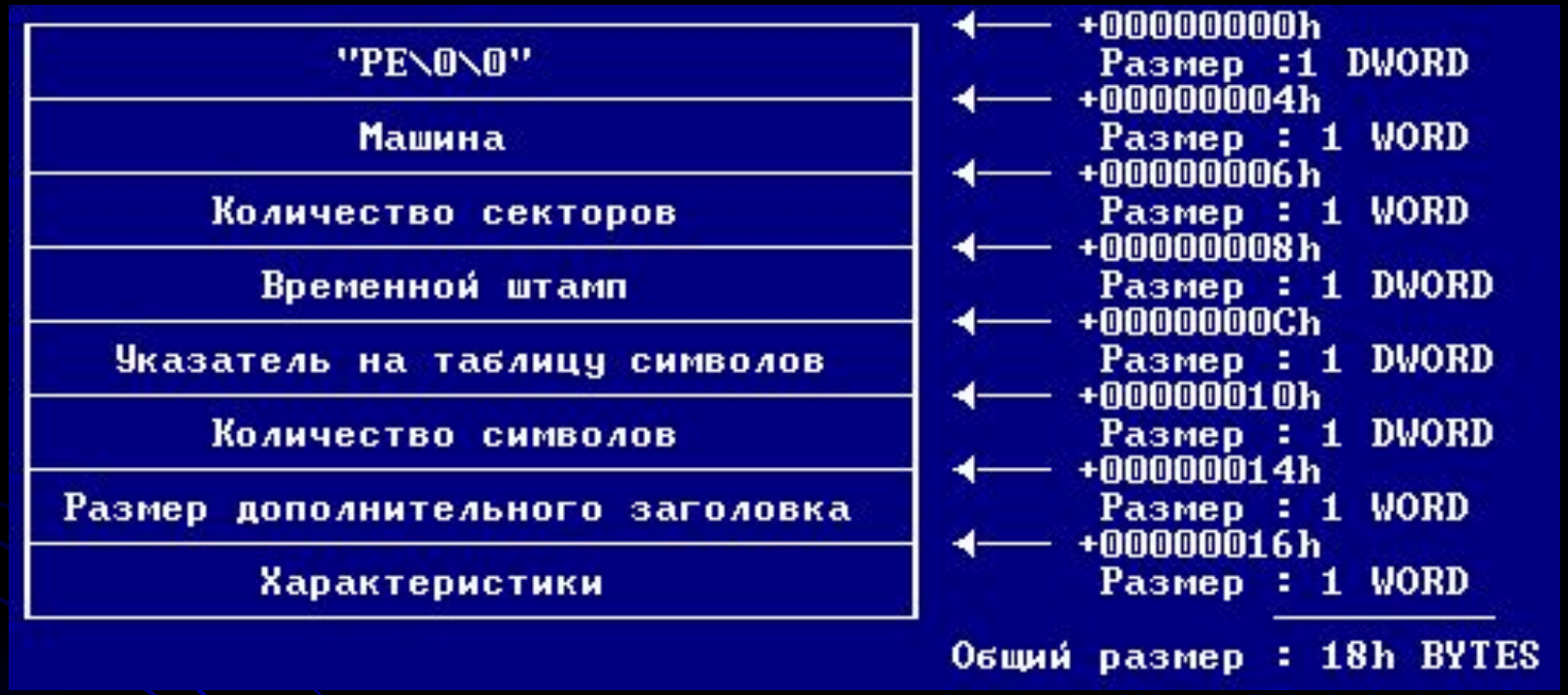
А.В. Неверов

Формат PE

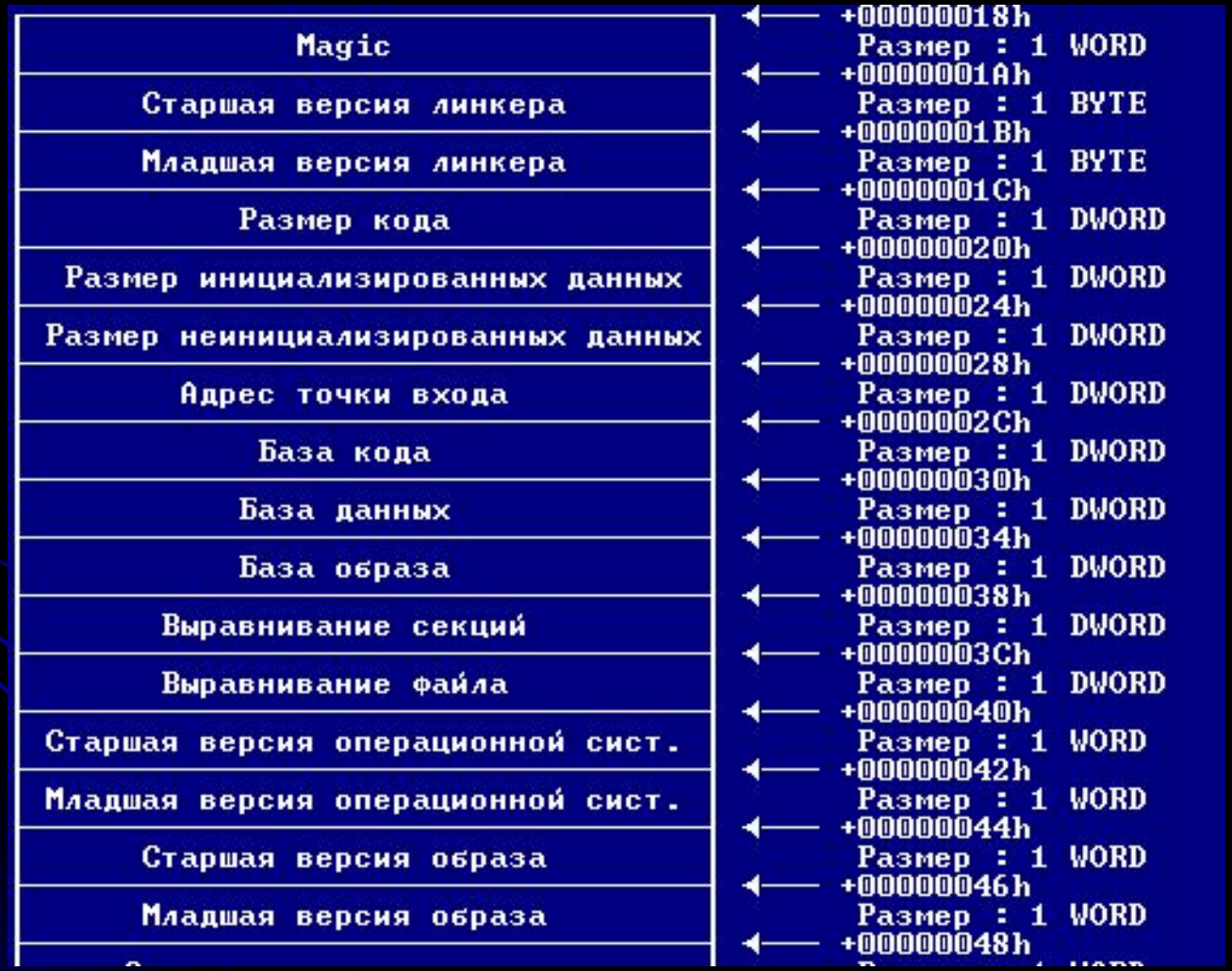

DOS stub
PE stuff
OFFSET = 00000000h
OFFSET = [DOS Stub+3Ch]


Совместимый с DOS заголовок EXE
Не используется
Идентификатор OEM
OEM-информация
Смещение на PE-заголовок
DOS-стаб и таблица релокейшенов
Не используется
PE-хедер (IMAGE_FILE_HEADER)
PE-хедер (IMAGE_OPTIONAL_HEADER)
Таблица секций
Секции
База заголовка образа
Не интересно (DOS-совместимость)
Очень интересно
Очень-очень интересно :)

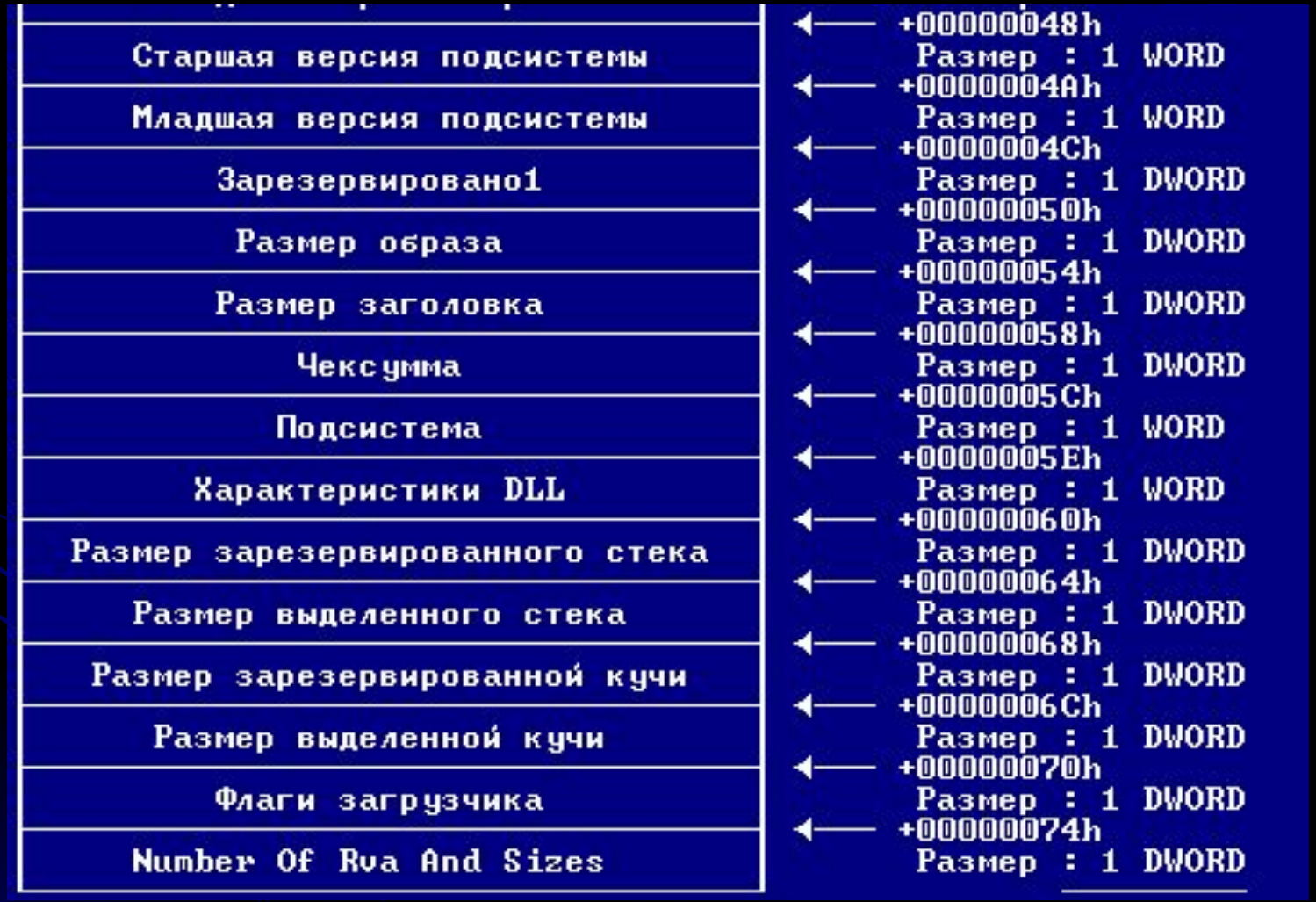
IMAGE_FILE_HEADER



IMAGE_OPTIONAL_HEADER

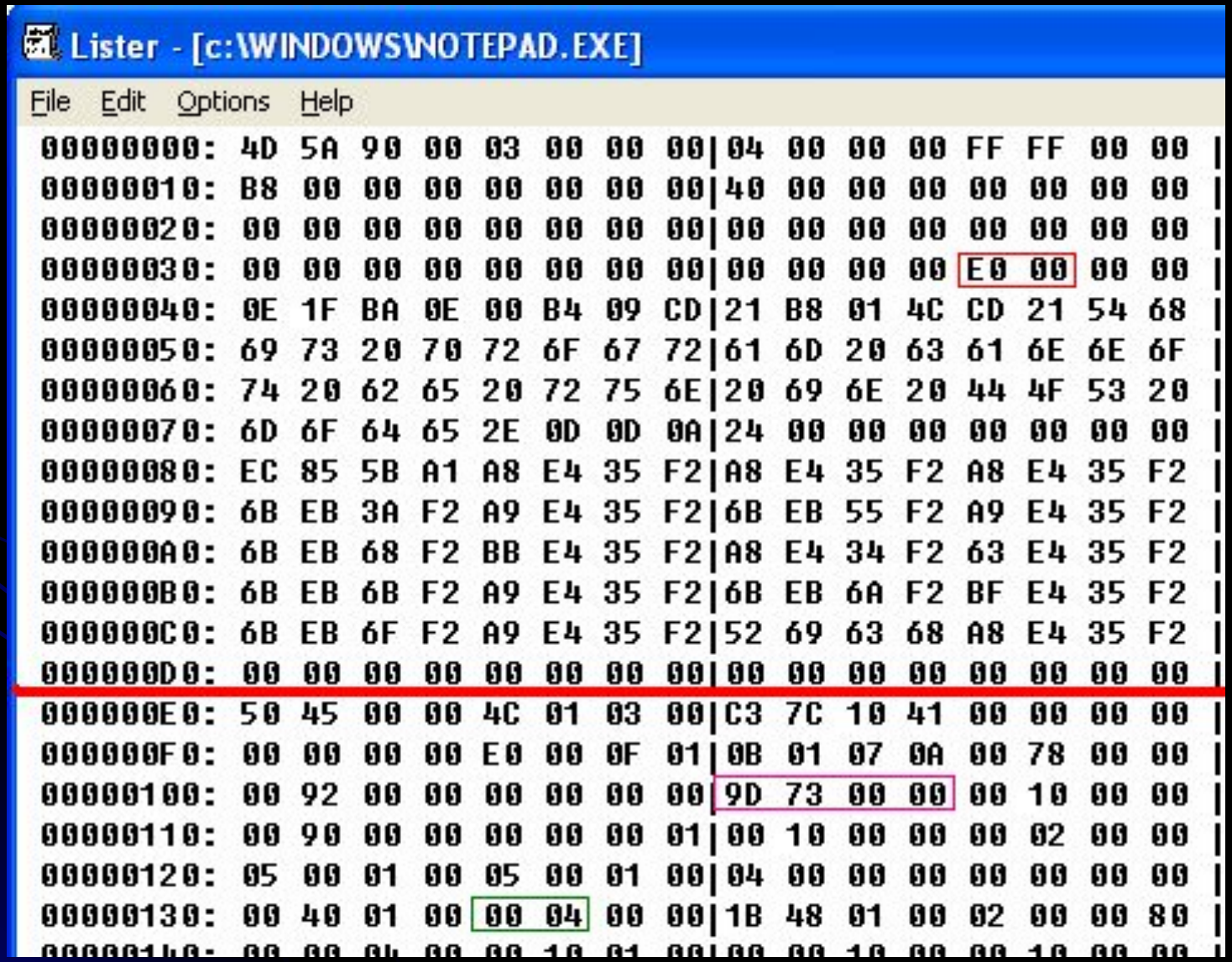


IMAGE_OPTIONAL_HEADER



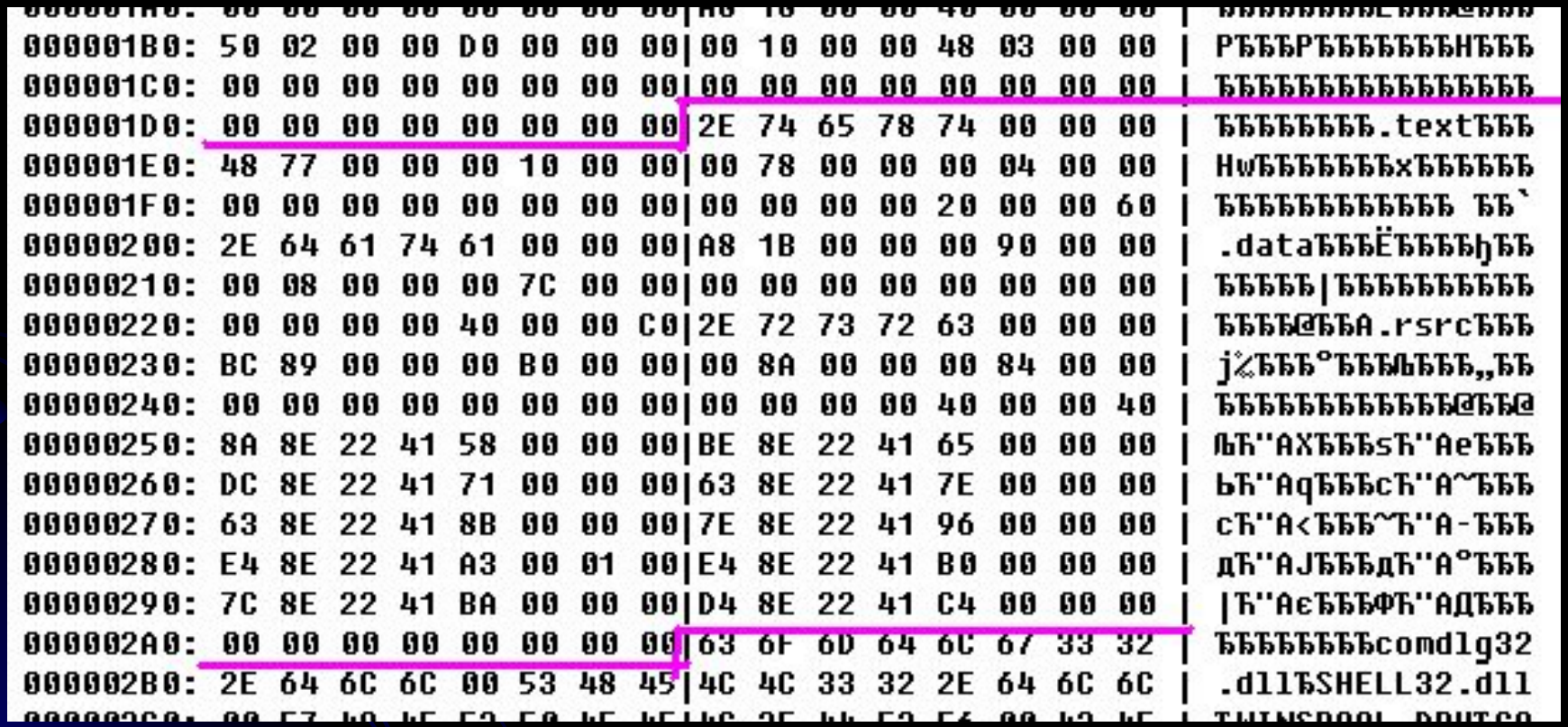
IMAGE_SECTION_HEADER

Notepad.exe


Lister - [c:\WINDOWS\NOTEPAD.EXE]
File Edit Options Help
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00
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 E0 00 00 00
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00
00000080: EC 85 5B A1 A8 E4 35 F2|A8 E4 35 F2 A8 E4 35 F2
00000090: 6B EB 3A F2 A9 E4 35 F2|6B EB 55 F2 A9 E4 35 F2
000000A0: 6B EB 68 F2 BB E4 35 F2|A8 E4 34 F2 63 E4 35 F2
000000B0: 6B EB 6B F2 A9 E4 35 F2|6B EB 6A F2 BF E4 35 F2
000000C0: 6B EB 6F F2 A9 E4 35 F2|52 69 63 68 A8 E4 35 F2
000000D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00
000000E0: 50 45 00 00 4C 01 03 00|C3 7C 10 41 00 00 00 00
000000F0: 00 00 00 00 E0 00 0F 01|0B 01 07 0A 00 78 00 00
00000100: 00 92 00 00 00 00 00 00|9D 73 00 00 00 10 00 00
00000110: 00 90 00 00 00 00 00 01|00 10 00 00 00 02 00 00
00000120: 05 00 01 00 05 00 01 00|04 00 00 00 00 00 00 00
00000130: 00 40 01 00 00 04 00 00|1B 48 01 00 02 00 00 80

Notepad.exe

Таблица секций



Потенциальные места заражения

- MZ-заголовок
- Секция кода (за счет расширения секции)
- Новая секция
- «Размазывание» вируса по свободным местам одной или нескольких секций)

Общий алгоритм заражения

- Открыть PE-exe файл
- Считать заголовок файла
- Добавить новую секцию
- Установить точку входа на новую секцию
- Дописать текст вируса по вычисленному физическому смещению в файл
- Записать измененный заголовок

Основные демаскирующие признаки

- Нетипичный стартовый код
- Наличие «опасных» и «кричащих» строк
- Наличие нестандартных секций