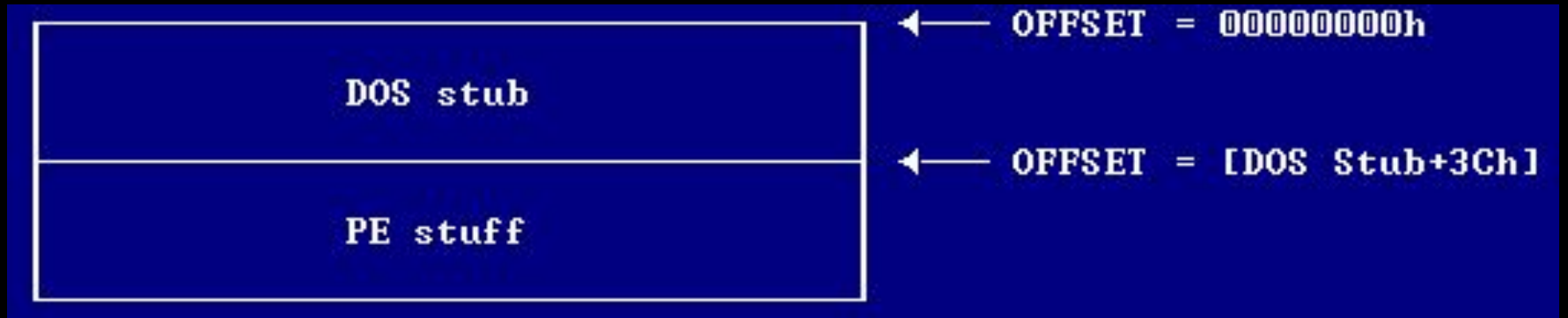


Вирусы для файлов в формате PE

А.В. Неверов



Формат PE



IMAGE_FILE_HEADER

"PE\0\0"	← +00000000h Размер : 1 DWORD
Машина	← +00000004h Размер : 1 WORD
Количество секторов	← +00000006h Размер : 1 WORD
Временной штамп	← +00000008h Размер : 1 DWORD
Указатель на таблицу символов	← +0000000Ch Размер : 1 DWORD
Количество символов	← +00000010h Размер : 1 DWORD
Размер дополнительного заголовка	← +00000014h Размер : 1 WORD
Характеристики	← +00000016h Размер : 1 WORD
Общий размер : 18h BYTES	

IMAGE_OPTIONAL_HEADER

Magic	← +000000018h Размер : 1 WORD
Старшая версия линкера	← +00000001Ah Размер : 1 BYTE
Младшая версия линкера	← +00000001Bh Размер : 1 BYTE
Размер кода	← +00000001Ch Размер : 1 DWORD
Размер инициализированных данных	← +000000020h Размер : 1 DWORD
Размер неинициализированных данных	← +000000024h Размер : 1 DWORD
Адрес точки входа	← +000000028h Размер : 1 DWORD
База кода	← +00000002Ch Размер : 1 DWORD
База данных	← +000000030h Размер : 1 DWORD
База образа	← +000000034h Размер : 1 DWORD
Выравнивание секций	← +000000038h Размер : 1 DWORD
Выравнивание файла	← +00000003Ch Размер : 1 DWORD
Старшая версия операционной сист.	← +000000040h Размер : 1 WORD
Младшая версия операционной сист.	← +000000042h Размер : 1 WORD
Старшая версия образа	← +000000044h Размер : 1 WORD
Младшая версия образа	← +000000046h Размер : 1 WORD
	← +000000048h Размер : 1 WORD

IMAGE_OPTIONAL_HEADER

Старшая версия подсистемы	← +00000048h Размер : 1 WORD
Младшая версия подсистемы	← +0000004Ah Размер : 1 WORD
Зарезервировано1	← +0000004Ch Размер : 1 DWORD
Размер образа	← +00000050h Размер : 1 DWORD
Размер заголовка	← +00000054h Размер : 1 DWORD
Чексумма	← +00000058h Размер : 1 DWORD
Подсистема	← +0000005Ch Размер : 1 WORD
Характеристики DLL	← +0000005Eh Размер : 1 WORD
Размер зарезервированного стека	← +00000060h Размер : 1 DWORD
Размер выделенного стека	← +00000064h Размер : 1 DWORD
Размер зарезервированной кучи	← +00000068h Размер : 1 DWORD
Размер выделенной кучи	← +0000006Ch Размер : 1 DWORD
Флаги загрузчика	← +00000070h Размер : 1 DWORD
Number Of Rva And Sizes	← +00000074h Размер : 1 DWORD

IMAGE_SECTION_HEADER

Имя секции	← Начало заголовка секции Размер : 8 BYTES
Виртуальный размер	← +000000008h Размер : 1 DWORD
Виртуальный адрес	← +00000000Ch Размер : 1 DWORD
Размер raw-данных	← +000000010h Размер : 1 DWORD
Указатель на raw-данные	← +000000014h Размер : 1 DWORD
Указатель на релокейшены	← +000000018h Размер : 1 DWORD
Указатель на номера строк	← +00000001Ch Размер : 1 DWORD
Количество релокейшенов	← +000000020h Размер : 1 WORD
Количество номеров строк	← +000000022h Размер : 1 WORD
Характеристики	← +000000024h Размер : 1 DWORD
Общий размер : 28h BYTES	

Notepad.exe

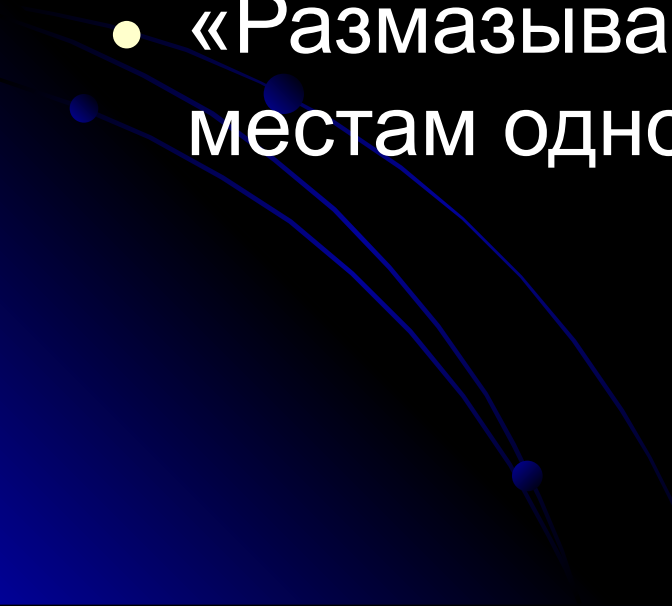
```
Lister - [c:\WINDOWS\notepad.exe]
File Edit Options Help
00000000: 4D 5A 90 00 03 00 00 00 | 04 00 00 00 FF FF 00 00
00000010: B8 00 00 00 00 00 00 00 | 40 00 00 00 00 00 00 00
00000020: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00
00000030: 00 00 00 00 00 00 00 00 | 00 00 00 00 E0 00 00 00
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
00000140: 00 00 00 00 00 10 01 00 | 00 00 10 00 00 10 00 00
```


Notepad.exe

Таблица секций

00000100:	00 00 00 00 00 00 00 00	00 00 00 00 40 00 00 00	РРРРРРРРРРРРРРРРРР
00000108:	50 02 00 00 00 00 00 00	00 10 00 00 48 03 00 00	РРРРРРРРРРРРРРРРРР
00000110:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	РРРРРРРРРРРРРРРРРР
00000118:	00 00 00 00 00 00 00 00	2E 74 65 78 74 00 00 00	РРРРРРРР.textРРРР
00000120:	48 77 00 00 00 10 00 00	00 78 00 00 00 04 00 00	НwРРРРРРРРxРРРРРР
00000128:	00 00 00 00 00 00 00 00	00 00 00 00 20 00 00 60	РРРРРРРРРРРР РР`
00000130:	2E 64 61 74 61 00 00 00	A8 1B 00 00 00 90 00 00	.dataРРРРРРРРРР
00000138:	00 08 00 00 00 7C 00 00	00 00 00 00 00 00 00 00	РРРРРР РРРРРРРРРР
00000140:	00 00 00 00 40 00 00 C0	2E 72 73 72 63 00 00 00	РРРР@РРРA.rsrcРРРР
00000148:	BC 89 00 00 00 B0 00 00	00 8A 00 00 00 84 00 00	j%РРРР°РРРРРРРР,,РР
00000150:	00 00 00 00 00 00 00 00	00 00 00 00 40 00 00 40	РРРРРРРРРРРРРР@РР
00000158:	8A 8E 22 41 58 00 00 00	BE 8E 22 41 65 00 00 00	РР"AXРРРРsР"АeРРРР
00000160:	DC 8E 22 41 71 00 00 00	63 8E 22 41 7E 00 00 00	РР"AqРРРРcР"А~РРРР
00000168:	63 8E 22 41 8B 00 00 00	7E 8E 22 41 96 00 00 00	cР"AcРРРР~Р"А-РРРР
00000170:	E4 8E 22 41 A3 00 01 00	E4 8E 22 41 B0 00 00 00	dР"AJРРРРdР"А°РРРР
00000178:	7C 8E 22 41 BA 00 00 00	D4 8E 22 41 C4 00 00 00	Р"AcРРРРФР"AdРРРР
00000180:	00 00 00 00 00 00 00 00	63 6F 6D 64 6C 67 33 32	РРРРРРРРcomd1g32
00000188:	2E 64 6C 6C 00 53 48 45	4C 4C 33 32 2E 64 6C 6C	.dllРSHELL32.dll
00000190:	00 57 40 4E 50 50 4E 4E	40 2F 44 50 56 00 40 4E	THINGSPOOL.DRIVER

Потенциальные места заражения

- MZ-заголовков
 - 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

