March 1990 ISSN 0956-9979

VIRUS BULLETIN

THE AUTHORITATIVE INTERNATIONAL PUBLICATION
ON COMPUTER VIRUS PREVENTION,
RECOGNITION AND REMOVAL

Editor: **Edward Wilding**

Technical Editor: **Fridrik Skulason**, University of Iceland

CONTENTS

EDITORIAL

Joseph Lewis Popp Arrested

On 18th January 1990 the Computer Crime Unit of the City and Metropolitan Police applied at Bow Street Magistrates Court, London, for a warrant for the arrest of Dr. Joseph Lewis Popp, an American citizen, on charges of blackmail in connection with the AIDS Information Diskette extortion bid. A Federal Fugitive Arrest Warrant for Popp's apprehension was issued six days later by U.S. District Judge Ann Aldrich. At 9.00 pm GMT on 1st February, the FBI and officers from the local sheriff's department arrested Popp at his parents' home in W. Willowick Drive, Willowick, Ohio, USA.

Popp, 39, appeared before U.S. Magistrate Joseph W. Bartunek of the Cleveland District Court on Friday 2nd February. He faces extradition proceedings under a 1972 treaty between the USA and the United Kingdom. When read the charges, Popp replied that he understood them but said "I don't understand how they apply in my case". Bail was refused. Psychiatric reports were ordered by Bartunek after John P. Kilroy, Popp's attorney described his client as "depressed and possibly suicidal".

Popp is a zoologist and anthropologist and has conducted research into animal behaviour for both UNICEF and the World Health Authority. He had researched into the connection between the AIDS/HIV biological virus and the African green monkey believed to have been the initial carrier of the disease and had also attended a number of WHO teaching courses in Africa. A 1972 biology graduate from Ohio State University, Popp went on to receive a doctorate in anthropology from Harvard University in 1979. Popp had worked on a WHO contract in Nairobi during December 1989 and returned to live with his parents, Joseph and Dorothy, upon its conclusion just before Christmas.

Popp denies being a director, shareholder, or employee of the PC Cyborg Corporation and says that he had no financial interest in the company. Kilroy quoted his client as saying "the sole reason for the project [the AIDS disk] was to use computers to provide health education to people around the world to fight the global epidemic of AIDS. I never made a penny out of this and I never intended to". Kilroy said that the disk's reported side effects were inexplicable but that the disks themselves were intended to generate money to conduct research into the AIDS biological virus. Popp claims that he received no money to distribute the disk and said that WHO officials were directors of the PC Cyborg Corporation and that the AIDS Information Diskettes were part of a secret plot to raise funds. Kilroy said that Popp was "certain that they're WHO officials going to deny any knowledge of participation". Popp said that PC Cyborg directors were aliases. The company's directors have been listed as Kitain Mekonen, Asrat Wakjira and Fantu Mekease while a fourth man, a Mr. E. Ketema, is also believed to be implicated. Ketema contacted the London circulation department of *PC Business World* in October of last year and purchased 7,000 address labels of which were used to mail the AIDS Trojan. Detective Inspector John Austen of New Scotland Yard's Computer Crime Unit has not revealed whether there are any suspects other than Popp.

World Health Organisation officials denied Popp's allegation. Thomas W. Netter, a WHO spokesman described the allegation as "totally and completely false" while both Dr. Mandel, director of computerisation at the WHO's Geneva headquarters and Salah Mandil, director of WHO's worldwide computer and telecommunications operations refuted Popp's claims. The WHO global program on AIDS employs 250 people and has a budget this year of $109 million. A mailing list containing 3,500 names from the WHO database was used to mail the AIDS Trojan.

FBI spokesman Bob Hawk said that the FBI had information that Popp was prepared to mail a further two million disks. The FBI's role had been to locate and apprehend the suspect while the detective work had been undertaken exclusively by the UK's Computer Crime Unit. Popp faces a maximum sentence of fourteen years' imprisonment for each count of blackmail. Extradition, if granted, is expected to take ten weeks to complete.

The charge: *That on 11th December 1989, within the jurisdiction of the Central Criminal Court, you with a view to gain for another, vis PC Cyborg Corporation of Panama, with menaces made unwarranted demand, vis a payment of one hundred and eighty nine U.S. dollars or three hundred and seventy eight U.S. dollars from the victim.*

Extradition and Blackmail

The law of extradition is fulginous and complex, although provisions of the Criminal Justice Act 1988 have clarified parts. The return of Dr. Popp will be governed principally by the treaty of 1972, as amended, between the USA and the UK. The UK has specified extradition for the offence of blackmail. However, should he be acquitted of blackmail the prosecution could still proceed afresh with other charges, e.g. criminal damage, so long as the particulars furnished to the US Court for the extradition disclosed them.

Blackmail requires the prosecution to show the demand was unwarranted, and that the menaces in support of it would make an ordinary person accede to the demand unwillingly. The defence may argue that the demands were contractual. However, warnings have been judged as menaces. Also, the business user who 'sees' his files but cannot use them may take little pressure to accede. Perhaps of more interest, there may be some dispute as to whether the unusable computer could be further harmed, and thus what the menace was. Further, there may be arguments about Dr. Popp's standards and beliefs by which the reasonableness of his conduct should be judged. This will be a matter for the jury.

Owen Keane

MAC THREATS

David Ferbrache

WDEF Usurps nVIR

All indications are that the WDEF virus reported on December 3rd 1989 (*see Virus Bulletin, January 1990, pp 14.*) is now rivalling the nVIR virus for the dubious title of most common Macintosh virus. The *Virus-L* electronic discussion forum has carried dozens of reports of the virus from the USA, Canada, Ireland and the UK. It seems clear that the virus has been spreading for some considerable time prior to detection. The virus' method of re-vectoring the resource manager traps to point to the ROM version of the routines has proved highly effective in evading detection.

The WDEF-A virus has now been reported from a number of locations in the UK. *MacUser* magazine reported a particularly serious incident in its February edition noting that over 2,000 infected disks had been reported as part of a free mailing of fonts with Issue 2 of the *MacPublishing* magazine. MacPublishing's management responded quickly by distributing an updated version of the public domain ant-viral program Disinfectant (versions 1.5 and 1.6 **will** detect WDEF).

A limited number of reports of WDEF-B infection have been received (a debugging version of WDEF-A which beeps on desktop infection) from four North American universities.

It is important to note that WDEF replicates via the desktop file on disk, and as such can infect disks containing no executable applications. In the case of the *MacPublishing* infection WDEF was transferred via a disk containing a hypertext stack from the USA. Re-infection from archive disks is posing significant problems at those institutions which do not use up-to-date anti-viral tools.

Mac Trojan Warning

Two new Trojan horses have been reported recently (February 4th, 1990) which affect the Apple Macintosh. The first is embedded in the program '*Mosaic*', the second in a *Stuffit*! archive containing '*FontFinder*'.

The first strain when launched will destroy the directories of all unlocked drives, renaming each destroyed drive as 'Gotcha!'. Unmounted hard drives are also attacked.

Damage appears to be restricted to destruction of directory information including file type and creator. Commercial data recovery utilities can normally restore the file structure.

The second strain displays a list of font styles and point sizes in the system file. On, or after, 10th February 1990 it will trigger destroying the directory structure in a similar manner to strain 1.

All indications are that these Trojans (first reported at the University of Alberta, Canada) are closely related in their destructive code and are assumed to have been released by the same person.

The characteristics of the two Trojan programs are:

```
Mosaic      Type=APPL, Creator=????
            Created 8/1/90 12:28am, modified 8/1/90
            1:27am (reported)
            Two code resources
                                CODE 0 32 bytes
                                CODE 1 6528 bytes

FontFinder  Type=APPL, Creator=BNBW
            Created 9/1/90 10:20pm, modified 9/1/90
            10:24pm
            Two code resources
                                CODE 0 32 bytes
                                CODE 1 12052 bytes
```

The Trojans contain readable text at the end of CODE 1, extracts are as follows:

```
Mosaic DEATHTRA DeathTrak II...
FontFinder KILLIT A Program modifications courtesy of
the Data Terror Group, CT, USA...You have been hit
by another DeathTrak system...
```

The text and code indicate the Trojans are related. The original reporter has proposed the following Virus Detective scan string:

```
Resource CODE & ID=1 & Data 44656174685472616B
```

This is a crude string but will identify both these Trojans.

Preventing Trojan Activity

As with resource manager traps on the Mac, it is possible to intercept a number of the operating system traps connected with low level disk activity. An obvious example is trap A9E9 hex which is the entry point to the disk initialisation library package (in particular the *DiZero* and *DiFormat* calls). By intercepting this trap (through the use of a protection INIT) the user can be supplied with a prompt as to whether the initialisation process can continue.

An example of such a protection INIT is the SAM intercept configured in advanced protection mode which will detect alterations to: *volume boot blocks; volume information; volume bit map on HFS volumes; volume block map on MFS volumes; volume b-trees on HFS volumes; volume directory on MFS volumes.*

Utilities such as the public domain Virus Blockade (Jeff Shulman) are also potentially effective against Trojan activity. This utility operates by over-writing a drive or component of a drive in software by trap interception. It should be noted that while protection INITs are an interim solution, it is possible for a Trojan to directly manipulate the underlying disk controller or to remove the patch to the trap table. **In general until computer systems incorporate the concept of a privileged operating system kernel with well defined entry points (supported by hardware protection and memory management), Trojans will be a major problem.**

IBM PC VIRUSES

This is a list of the known viruses affecting IBM PCs and compatibles, including XTs, ATs and PS/2s. The first part of the list gives aliases and brief descriptions of viruses which have been seen, while the second part lists viruses which have been reported.

Each entry consists of the virus group name, its aliases and the virus type (See “Type codes” table). This is followed by a short description (if available) and a 10 to 16 byte hexadecimal pattern which can be used to detect the presence of the virus by the “search” routine of disk utility programs such as The Norton Utilities or your favourite disk scanning program. Offset normally means the number of bytes from the virus entry point. For parasitic viruses, the infective length (the amount by which the length of an infected file has increased) is also given.

Type codes:

C = Infects COM files
E = Infects EXE files
D = Infects DOS boot sector (Logical sector 0 on hard and floppy disks)
M = Infects disk boot sector (Absolute sector 0 on hard disk, Logical sector 0 on floppy)
N = Not memory-resident after infection
R = Memory-resident after infection

SEEN VIRUSES

405 - CN: Infects one COM file (on a different disk) each time an infected program is run by overwriting the first 405 bytes. If the length of the file is less than 405 bytes, it will be increased to 405. The virus only infects the current directory and does not recognise a file already infected.

```
405              26A2 4902 26A2 4B02 26A2 8B02 50B4 19CD ; Offset 00A
```

1260 - CN: 1260 infects COM files, adding 1260 bytes to them. The first 39 bytes contain code used to decrypt the rest of the virus. A variable number of short (irrelevant) instructions are added between the decoding instructions at random in an attempt to prevent virus scanners from using identification strings. **No search pattern is possible.** *(VB Mar 90)*

4K, 4096, IDF, Israeli Defence Forces - CER: Infective length is 4096 bytes. Virus awaiting disassembly.

```
4K               E808 0BE8 D00A E89A 0AE8 F60A E8B4 0A53 ; Offset 239
```

Alabama - ER: Infective length is 1560 bytes. Virus awaiting disassembly.

```
Alabama          8CDD 33DB 8EDB 8B07 0B47 0274 7489 1F89 ; Offset 109
```

Amstrad - CN: Adds 847 bytes to the front of any COM file in the current directory. The virus is only 334 bytes long, which makes it the shortest PC virus known. The rest contains an advertisment for Amstrad computers.

```
Amstrad          C706 0E01 0000 2E8C 0610 012E FF2E 0E01 ; Offset 114
```

Brain, Ashar, Shoe - DR: Consists of a bootstrap sector and 3 clusters (6 sectors) marked as bad in the FAT. The first of these contains the original boot sector. In its original version it only infects 360K floppy disks and occupies 7K of RAM. It creates a label “(c) Brain” on an infected disk. There is a variation which creates a label “(c) ashar”.

```
Brain            A006 7CA2 097C 8B0E 077C 890E 0A7C E857 ; Offset 158
```

Cascade, Fall, Russian - CR: This encrypted virus attaches itself to the end of a COM file, increasing its length by 1701 or 1704 bytes. The encryption key includes the length of the infected program, so infected files of different lengths will look different. After infection it becomes memory-resident and infects every COM file executed, including COMMAND.COM. The original version will produce a “falling characters” display if the system date is between 1st October and 31st December 1988. The formatting version will format the hard disk on any day between 1st October and 31st December of any year except 1993. Both activations occur a random time after infection with a maximum of 5 minutes. *(VB Sep 89)*

```
Cascade (1) 01   0F8D B74D 01BC 8206 3134 3124 464C 75F8 ; Offset 012, 1701 bytes, Falling characters
Cascade (1) 04   0F8D B74D 01BC 8506 3134 3124 464C 75F8 ; Offset 012, 1704 bytes, Falling characters
Cascade (1) Y4   FA8B CDE8 0000 5B81 EB31 012E F687 2A01 ; Offset 000, 1704 bytes, Falling characters
Cascade format   0F8D B74D 01BC 8506 3134 3124 464C 77F8 ; Offset 012, 1704 bytes, Formats hard disk
```

Dark Avenger - CER: Appears to infect on file open and close as well as load and execute expanding the file by 1800 bytes. This means that a virus-scan program will cause it to infect every program on the disk. Only infects if program is at least 1775 bytes. May overwrite data sectors with garbage. There is a variant which extends the file by 2000 bytes. *(VB Feb 90)*

```
Dark Avenger     A4A5 8B26 0600 33DB 53FF 64F5 E800 005E ; Offset variable
```

Datacrime - CN: The virus attaches itself to the end of a COM file, increasing its length by 1168 or 1280 bytes. On execution of an infected program, the virus searches through full directory structure of drives C, D, A and B for an uninfected COM file which will be infected. Files with 7th letter D will be ignored (including COMMAND.COM). If the date is on or after 13th October of any year, the first 9 tracks of the hard disk will be formatted. The format is low level after displaying the message:

```
DATACRIME VIRUS
RELEASED: 1 MARCH 1989
```

This message is stored in an encrypted form in the virus. *(VB Aug 89).*

```
Datacrime (1)     3601 0183 EE03 8BC6 3D00 0075 03E9 0201 ; Offset 002, 1168 bytes
Datacrime (2)     3601 0183 EE03 8BC6 3D00 0075 03E9 FE00 ; Offset 002, 1280 bytes
```

Datacrime II - CEN: This encrypted virus attaches itself to the end of a COM or EXE file, increasing their length by 1514 bytes. The virus searches through the full directory structure of drives C, A and B for an uninfected COM or EXE file. It ignores any file if the second letter is B. If the date is on or after 13th October of any year, but not a Monday, a low level format of the first 9 tracks will be done on the hard disk after displaying the message:

```
DATACRIME II VIRUS
```

This message is stored in an encrypted form in the virus.

```
Datacrime II      2E8A 072E C605 2232 C2D0 CA2E 8807 432E ; Offset 022, 1514 bytes
```

dBASE - CR: Transposes bytes in dBASE files (DBF). Creates the hidden file BUGS.DAT in the root directory of drive C: and generates errors if the absolute difference between the month of creation of BUGS.DAT and the current month is greater or equal to 3. Infective length is 1864 bytes. The destroy version destroys drives D: to Z: when the trigger point is reached. *(VB Dec 89)*

```
dBASE             50B8 0AFB CD21 3DFB 0A74 02EB 8A56 E800 ; Offset 636, 1864 bytes
dBASE destroy     B900 01BA 0000 8EDA 33DB 50CD 2658 403C ; Offset 735, 1864 bytes
```

December 24th - ER: A mutation of the Icelandic (3) virus. It will infect one out of every 10 EXE files run, which grow by 848-863 bytes. If an infected file is run on December 24th, it will stop any other program from running and display the message “Gledileg jol” (Merry Christmas in Icelandic).

```
December 24th     C606 7E03 FEB4 5290 CD21 2E8C 0645 0326 ; Offset 044
```

Den Zuk, Search - DR: The majority of the virus is stored in a specially formatted track 40, head 0 sectors 33 to 41. When Ctrl-Alt-Del is pressed, the virus intercepts it and displays “DEN ZUK” sliding in from the sides of the screen. This does not happen if KEYBUK or KEYB is installed. Den Zuk will remove Brain and Ohio and replace them with copies of itself.

```
Den Zuk           FA8C C88E D88E D0BC 00F0 FBB8 787C 50C3 ; Offset 0
```

Devil’s Dance - CR: A simple virus which infects COM files, adding 951 bytes at the end of infected files. The virus is believed to have originated in Spain or Mexico.

```
Devil's Dance     B800 0150 8CC8 8ED8 8EC0 C306 B821 35CD ; Offset 011
```

Disk Killer, Ogre - DR: The virus infects floppy and hard disks and if the computer is left on for more than 48 hours, it will encrypt the contents of the bootable disk partition. The infection of a disk occurrs by intercepting a disk read - INT 13H function 2. When the virus triggers, it displays the message “Disk Killer — Version 1.00 by Ogre Software, 04/01/1989. Warning !! Don’t turn off the power or remove the diskette while Disk Killer is Processing!”. *(VB Jan 90)*

```
Disk Killer       2EA1 1304 2D08 002E A313 04B1 06D3 E08E ; Offset 0C3
```

Do-nothing - CR: A badly written virus from Israel that assumes a 640K system.

```
Do nothing        8CCA 8EDA BA00 988E C2F3 A41E B800 008E ; Offset 020
```

Eddie-2 - CER: A non-destructive virus from Bulgaria. It marks infected files with a value of 62 in the seconds field of the timestamp, which makes them immune from infection by Vienna or Zero Bug. Infected files grow by 651 bytes, but this will not be seen if a DIR command is used - the virus intercepts the find-first and find-next functions, returning the correct (uninfected) length.

```
Eddie-2           D3E8 408C D103 C18C D949 8EC1 BF02 00BA ; Offset 02D, 651 bytes
```

E.D.V. - DR: E.D.V. marks infected disks with “EV” at the end of the boot sector and stores the original boot sector code in the last sector of the last track on 360K disks, just like the Yale virus. Virus awaiting full disassembly.

```
E.D.V.            0C01 5083 EC04 B800 01CF B601 B908 2751 ; Offset 0C1
```

Fu Manchu - CER: The virus attaches itself to the beginning of a COM file or to the end of an EXE file. Infective length is 2086 bytes (COM) and 2080 (EXE). It is a rewritten version of the Jerusalem virus, but the marker is now “rEMHOr” and the preceding “sU” is now “sAX” (Sax Rohmer, creator of Fu Manchu). After installing itself as memory-resident, it will infect any COM or EXE file, except COMMAND.COM. EXE files are infected only once, unlike the original Jerusalem. One in sixteen times on infection a timer is installed, which will trigger a display “The world will hear from me again” after a random number of half-hours (max. 7.5 hours). The machine then reboots. The same message is also displayed on pressing Ctrl-Alt-Del, but the virus does not survive the reboot. If the date is after 1st August 1989, the virus monitors the keyboard buffer and adds derogatory comments to the names of politicians (Thatcher, Reagan, Botha and Waldheim), overstrikes two four-letter words, and displays “virus 3/10/88 - latest in the new fun line!” if “Fu Manchu” is typed. All messages are encrypted. *(VB Jul 89)*

```
Fu Manchu          FCB4 E1CD 2180 FCE1 7316 80FC 0472 11B4 ; Offset 1EE, 2086 bytes COM, 2080 bytes EXE
```

GhostBalls - CN: A strain of Vienna virus. Seconds field changed to 62, as in Vienna. Infective length is 2351 bytes and the virus attaches itself to the end of the file. When run, it will infect other COM files and try to place a modified copy of the Italian virus into boot sector of drive A:. This copy of the Italian runs on 286 machines but is non-infective. Virus contains text “GhostBalls, Product of Iceland”.

```
GhostBalls         AE75 EDE2 FA5E 0789 BC16 008B FE81 C71F ; Offset 051
```

Hallochen - CER: A virus which reputedly originated in West Germany. It contains two text strings (o in Hallochen has an umlaut (character code 148 decimal)):

```
     Hallochen !!!!!!, Here I’m..
     Acrivate Level 1..
```

The virus will not infect “old” files. If the value of the month or year fields in the time stamp is different from the current date, the file will not be infected. The virus will only infect files longer than 5000 bytes, increasing their length by 2011 bytes.

```
Hallochen          EB8C C903 D98E D3BC DB08 53BB 2E00 53CB ; Offset 01E, 2011 bytes
```

Icelandic, Saratoga - ER: The virus attaches itself at the end of an EXE file and after becoming memory-resident, it will infect only one in ten (one in two for the Icelandic (2) variant) programs executed. When a program is infected, the disk is examined and if it has more than 20 MBytes, one cluster is marked as bad in the first copy of the FAT. There is a mutation which does not flag clusters. Version (1) will not infect the system unless INT 13H segment is 0700H or F000H, thus avoiding detection by anti-virus programs which hook into this interrupt. Version (3) does not flag clusters and bypasses all interrupt-checking programs.

```
Icelandic (1)      2EC6 0687 020A 9050 5351 5256 1E8B DA43 ; Offset 0C6, 656 bytes
Icelandic (2)      2EC6 0679 0202 9050 5351 5256 1E8B DA43 ; Offset 0B8, 642 bytes
Icelandic (3)      2EC6 066F 020A 9050 5351 5256 1E8B DA43 ; Offset 106, 632 bytes
```

Italian, Pingpong, Turin, Bouncing Ball, Vera Cruz - DR: The virus consists of a boot sector and one cluster (2 sectors) marked as bad in the first copy of the FAT. The first sector contains the rest of the virus while the second contains the original boot sector. It infects all disks which have at least two sectors per cluster and occupies 2K of RAM. It displays a single character “bouncing ball” if there is a disk access during the one-second interval in any multiple of 30 minutes on the system clock. The original version will hang when run on an 80286 or 80386 machine, but a new version has been reported which runs normally. If a warm boot is performed after the machine hangs, an uninfected disk will still become infected. *(VB Nov 89)*

```
Italian-Gen        B106 D3E0 2DC0 078E C0BE 007C 8BFE B900 ; Offset 030
Italian            32E4 CD1A F6C6 7F75 0AF6 C2F0 7505 52E8 ; Offset 0F0
```

Jerusalem, PLO, Friday the 13th, Israeli - CER: The virus attaches itself to the beginning of a COM file or at the end of an EXE file. When an infected file is executed, the virus becomes memory-resident and will infect any COM or EXE program run, except COMMAND.COM. COM files are infected only once, while EXE files are re-infected every time that they are run. Infective length is 1813 bytes (COM) and 1808 bytes (EXE). The virus finds the end of EXE files from the information in the file header, and if this is less than the actual file length, the virus will overwrite part of the file. After the system has been infected for 30 minutes, row 5 column 5 to row 16 column 16 on the screen are scrolled up two lines, creating a “black window”. The system then slows down, due to a time-wasting loop installed on each timer interrupt. If the system is infected when the date is set to 13th of any month which is also a Friday, every program run will be deleted. *(VB Jul 89)*

```
Jerusalem          03F7 2E8B 8D11 00CD 218C C805 1000 8ED0 ; Offset 0AC, 1813 bytes COM, 1808 bytes EXE
```

Lehigh - CR: The virus only infects COMMAND.COM. It is 555 bytes long and becomes memory-resident when the infected copy is run. If a disk is accessed which contains an uninfected COMMAND.COM, the copy is infected. A count of infection generation is kept inside the virus, and when it reaches 4 (or 10 in a mutated version), the current disk is trashed each time a disk is infected, provided that (a) the current disk is either in the A drive or B drive, (b) the disk just infected is either the A drive or B drive and (c) the disk just infected is not the current one. The trashing is done by overwriting the first 32 sectors following the boot sector. Infection changes the date and time of infected COMMAND.COM.

```
Lehigh             8B54 FC8B 44FE 8ED8 B844 25CD 2106 1F33 ; Offset 1EF
```

MachoSoft - CEN: Swaps every string “MicroSoft” with “MachoSoft” on the hard disk. Searches 20 sectors at a time, storing the last sector searched in IBMNETIO.SYS which is marked hidden and system. After searching the last sector it starts again. This will only happen after 1st January 1985 and if the environment variable VIRUS is not set to OFF. Infective length is 3550 to 3560 bytes. Random directory search for uninfected files. Infects COMMAND.COM. This virus is closely related to Syslock.

```
MachoSoft          5051 56BE 5900 B926 0890 D1E9 8AE1 8AC1 ; Offset ?
```

Mistake, Typoboot, Typo - DR: Exchanges letters for phonetically similar ones (for example “C” & “K”) while they are being output to the printer. Reportedly written in Israel. A mutation of the Italian virus with about 35 % of the code rewritten. The boot sector is almost identical to the Italian.

```
Mistake            32E4 CD1A 80FE 0376 0A90 9090 9090 52E8 ; Offset 0F0
```

MIX1 - ER: The virus infects only EXE files attaching itself to the end. When an infected program is run, the virus will copy itself to the top of the free memory. Some programs may overwrite this area, causing the machine to crash. The virus traps printer and asynch interrupts and corrupts traffic by substituting characters. 50 minutes after infection, the virus alters Num Lock and Caps Lock keyboard settings. 60 minutes after infection, a display similar to the Italian virus (bouncing ball) will be produced. The virus will infect every tenth program run. Infected files always end in “MIX1” and the infective length of MIX1 is 1618 to 1633 bytes and MIX1-2 1636 to 1651 bytes. *(VB Dec 89)*

```
MIX1             B800 008E C026 803E 3C03 7775 095F 5E59 ; Offset 02E
MIX1-2           B800 008E C0BE 7103 268B 3E84 0083 C70A ; Offset 02A
```

New Zealand, Stoned, Marijuana - MR: The virus consists of a boot sector only. It infects all disks and occupies 2K of RAM. On floppy disks, the sector 0 is infected, while on the hard disks the physical sector 0 (Master boot sector) is infected. The original boot sector is stored in track 0 head 1 sector 3 on a floppy disk and track 0 head 0 sector 2 on a hard disk. The boot sector contains two character strings: “Your PC is now Stoned!” and “LEGALISE MARIJUANA” but only the former one is displayed once in eight times, and only if booted from floppy disk. The version (2) stores the original boot sector at track 0 head 0 sector 7 on a hard disk. The second string is not transferred when a hard disk is infected. A mutation has been reported in Australia which also displays “LEGALISE MARIJUANA”.

```
New Zealand (1)  0400 B801 020E 07BB 0002 B901 0033 D29C ; Offset 043
New Zealand (2)  0400 B801 020E 07BB 0002 33C9 8BD1 419C ; Offset 041
```

Number of the Beast - CR: An advanced virus from Bulgaria, only 512 bytes long. The length of the file does not appear to increase since the virus overwrites the first 512 bytes of the programs it infects with itself, storing the original 512 bytes in the unused space of a disk cluster, after the logical end of file.

```
Number of Beast  5A52 0E07 0E1F 1EB0 5050 B43F CBCD 2172 ; Offset 0A3
```

Old Yankee - EN: This is the first of the viruses which play the “Yankee Doodle Dandy”. It only infects EXE files, increasing their length by 1961 bytes. When an infected program is run, it will infect a new file and then play the melody.

```
Old Yankee       B003 CF9C 3D00 4B74 069D 2EFF 2E00 0006 ; Offset variable, 1961 bytes
```

Oropax, Music virus - CR: Infected files increase by between 2756 & 2806 bytes. Total length becomes divisible by 51. 5 minutes after the infection, the virus plays three different tunes with a 7-minute interval. Does not infect COMMAND.COM.

```
Oropax           06B8 E033 CD21 3CFF 7423 8CCE 8EC6 8B36
```

Pentagon - DR: The virus consists of a boot sector and two files. The sample obtained does not work, but it contains the code which would survive a warm boot (Ctrl-Alt-Del). It could only infect 360K floppy disks, and will look for and remove Brain from any disk it infects. It occupies 5K of RAM.

```
Pentagon         8CC8 8ED0 BC00 F08E D8FB BD44 7C81 7606 ; Offset 037
```

Perfume - CR: The infected program will sometimes ask the user a question and not run unless the answer is 4711 (name of a perfume). The virus will look for COMMAND.COM and infect it. Infective length is 765 bytes.

```
Perfume          FCBF 0000 F3A4 81EC 0004 06BF BA00 57CB ; Offset 0AA
```

Pixel - CN: Pixel viruses are practically identical to the Amstrad virus, although they are shorter: 345 and 299 bytes. No side-effects are noticeable until the 5th generation is reached, at which stage there is a 50 % chance that the following message will appear when an infected program is executed:

```
        Program sick error: Call doctor or buy PIXEL for cure description
```

```
Pixel (1)        0E1F 2501 0074 4CBA D801 B409 CD21 CD20 ; Offset 0C8, 354 bytes
Pixel (2)        BA9E 00B8 023D CD21 8BD8 061F BA2B 01B9 ; Offset 033, 299 bytes
```

South African, Friday the 13th, Miami, Munich, Virus-B - CN: Infective length is 419 bytes, but some reports suggest between 415 and 544 bytes. Does not infect files with Read-Only flag set. Virus-B is a non-destructive mutation containing South African 2 pattern. COMMAND.COM is not infected. Every file run on a Friday 13th will be deleted.

```
South African 1  1E8B ECC7 4610 0001 E800 0058 2DD7 00B1 ; Offset 158
South African 2  1E8B ECC7 4610 0001 E800 0058 2D63 00B1 ; Offset 158
```

Suriv 1.01, April 1st COM - CR: A precursor to Jerusalem infecting only COM files with the virus positioned at the beginning of the file. Infective length is 897 bytes. If the date is 1st April, the virus will display “APRIL 1ST HA HA HA YOU HAVE A VIRUS” and the machine will lock. If the date is after 1st April 1988, the virus produces the message “YOU HAVE A VIRUS !!!” but the machine will not lock. The virus is memory resident and will not infect COMMAND.COM. *(VB Aug 89)*

```
Suriv 1.01       0E1F B42A CD21 81F9 C407 721B 81FA 0104 ; Offset 304, 897 bytes
```

Suriv 2.01, April 1st EXE - ER: A precursor to Jerusalem infecting only EXE files with the virus positioned at the beginning of the file. Infective length is 1488 bytes. If the date is 1st April, the virus will display “APRIL 1ST HA HA HA YOU HAVE A VIRUS”. If the year is 1980 (DOS default) or the day is Wednesday after 1st April 1988, the machine will lock one hour after infection. *(VB Aug 89)*

```
Suriv 2.01       81F9 C407 7228 81FA 0104 7222 3C03 751E ; Offset 05E, 1488 bytes
```

Suriv 3.00, Israeli - CER: An earlier version of Jerusalem infecting COM and EXE files and displaying the side-effects 30 seconds after infection instead of 30 minutes. Infective length is 1813 bytes (COM) and 1808 bytes (EXE). Program delete does not work. *(VB Aug 89)*

```
Suriv 3.00      03F7 2E8B 8D15 00CD 218C C805 1000 8ED0 ; Offset 0B0, 1813 COM, 1808 EXE
```

Swap - DR: Does not infect until ten minutes after boot. One bad cluster on track 39, sectors 6 & 7 (head unspecified). Uses 2K of RAM. Infects floppy disks only. Does not store the original boot sector anywhere. Virus creates a display similar to Cascade, but is transmitted via boot sector.

```
Swap            31C0 CD13 B802 02B9 0627 BA00 01BB 0020 ; Offset ?
```

Sylvia - CN: The virus displays the message "This program is infected by a HARMLESS Text-Virus V2.1", "Send a FUNNY postcard to: Sylvia Verkade, Duinzoom 36b, 3235 CD Rockanje, The Netherlands", "You might get an ANTIVIRUS program....." when an infected program is executed, but if the above text is tampered with, the (encrypted) message "F*** YOU LAMER !!!!", "system halted....$" will be displayed. When an infected program is run, the virus will look for 5 COM files on drive C: and the current drive. COMMAND.COM, IBMBIO.COM and IBMDOS.COM are not infected. The virus adds 1301 bytes to the beginning of the infected files and 31 bytes at the end.

```
Sylvia          CD21 EBFE C3A1 7002 A378 0233 C0A3 9E02 ; Offset 229
```

Syslock - CEN: This encrypted virus attaches itself to the end of a COM or an EXE file. Infective length is 3551 bytes. It infects a program one in four times when executed. Will not infect if environment contains SYSLOCK=@.

```
Syslock         8AE1 8AC1 3306 1400 3104 4646 E2F2 5E59 ; Offset 0, 3551 bytes
```

Traceback, Spanish - CER: This virus attaches itself to the end of a COM or an EXE file. Infective length is 3066 bytes. It becomes memory-resident when the first infected program is run and will infect any program run. If the date is 5th December or later, the virus will look for and infect one COM or EXE file either in the current directory or the first one found starting with the root directory. If the date is 28th December 1988 or later, the virus produces a display similar to Cascade one hour after infection. If nothing is typed, the screen restores itself after one minute. Display will repeat every hour. Spanish is an earlier version with a reported infective length of 2930 or 3031 bytes. *(VB Sep 89)*

```
Traceback       B419 CD21 89B4 5101 8184 5101 8408 8C8C ; Offset 104, 3066 bytes
Spanish         E829 06E8 E005 B419 CD21 8884 E300 E8CE ; Offset ?
```

Typo, Typo COM, Fumble - CR: Infects all COM files in the subdirectory on odd days of every month. If typing fast, substitutes keys with the ones adjacent on the keyboard. Infective length is 867 bytes.

```
Typo            5351 521E 0656 0E1F E800 005E 83EE 24FF ; Offset 01D, 867 bytes
```

Vacsina - CER: Infective length 1206 to 1221 bytes (COM) and 1338 to 1353 bytes (EXE). After a successful infection of a COM file, a bell is sounded. Infects any file loaded via INT 21 function 4B (load and execute), i.e. COM, EXE, OVL and APP (GEM) files. Checks version number of itself (current is 5) and replaces with newer code. A member of the "Bulgarian 50" (see Yankee).

```
Vacsina (1)     8CC8 8ED8 8EC0 8ED0 83C4 02B8 0000 502E ; Offset variable
Vacsina (2)     E800 005B 2E89 47FB B800 008E C026 A1C5 ; Offset variable
```

Valert - ?: This virus was by accident posted to the V-ALERT electronic mail list recently. Virus awaiting disassembly.

```
Valert          1E0E 1F8D 36F7 04BF 0001 B920 00F3 A42E ; Offset 0
```

Vcomm - ER: This virus first increases the length of infected programs so that it becomes a multiple of 512 bytes. Then it adds 637 bytes to the end of the file. The resident part will intercept any disk write and change it into a disk read.

```
Vcomm           80FC 0375 04B4 02EB 0780 FC0B 7502 B40A ; Offset 261
```

Vienna, Austrian, Unesco, DOS62, Lisbon - CN: The virus infects the end of COM files. Infective length is 648 bytes. It looks through the current directory and the directories in the PATH for an uninfected COM file. One file in eight becomes overwritten. Seconds stamp of an infected file is set to 62. A number of variants, shorter than the original, but functionally equivalent, have been reported in Bulgaria.

```
Vienna (1)      8BF2 83C6 0A90 BF00 01B9                ; Offset 005, 648 bytes
Vienna (2)      FC8B F281 C60A 00BF 0001 B903 00F3 A48B ; Offset 004, 648 bytes
Vienna (3)      FC89 D683 C60A 90BF 0001 B903 00F3 A489 ; Offset 004
Vienna (4)      FC8B F283 C60A BF00 01B9 0300 F3A4 8BF2 ; Offset 004, 623 bytes
Vienna (5)      CD21 0E1F B41A BA80 00CD 2158 C3AC 3C3B ; Offset variable
Vienna (6)      8E1E 2C00 AC3C 3B74 093C 0074 03AA EBF4 ; Offset variable
```

Virus-90 - CN: The author of this virus is Patrick A. Toulme. He uploaded the virus to a number of Bulletin Boards, stating that the source was available for $20. When an infected program is run it will display the message "Infected", infect a COM file in drive A: and display the message "Done". Infective length is 857 bytes.

```
Virus-90        558B 2E01 0181 C503 0133 C033 BBB9 0900 ; Offset 01E
```

W13 - CN: A primitive group of viruses which originated in Poland. They have no known side-effects and there are two variants, 534 and 507 bytes long. The variant with 507 bytes has some bugs corrected.

```
W13             8BD7 2BF9 83C7 0205 0301 03C1 8905 B440 ; Offset variable
```

Yale, Alameda, Merritt - DR: This virus consists of a boot sector and infects floppies in A drive only. It becomes memory-resident and occupies 1K of RAM. The original boot sector is held in track 39 head 0 sector 8. The machine will hang if the virus is run on an 80286 or 80386 machine. If a warm boot is performed after the machine hangs, an uninfected disk will still become infected. It has been assembled using A86 and contains code to format track 39 head 0, but this is not accessed. Survives a warm boot.

```
Yale          BB40 008E DBA1 1300 F7E3 2DE0 078E C00E ; Offset 009
```

Yankee - CER: Infective length 2885 bytes. Virus awaiting disassembly. This is a member of the “Bulgarian 50” group of viruses, which consists of some 50 related variants, all written by the same person. Vacsina is the other member of the group. All the viruses in the group are reported to remove infections by older variants, and the size is varying from 1200 to 3500 bytes.

```
Yankee        0000 7402 B603 520E 5143 CFE8 0000 5B81 ; Offset variable
```

Zero Bug, Palette - CR: Infective length is 1536, attachs to beginning of COM file. The virus modifies the number of seconds to 62 (like Vienna). If the virus is active in memory and the DIR command is issued, the file length of infected files will be identical to that before the infection. A mutation called Palette (infective length 1536 bytes) has also been reported.

```
Zero Bug      81C9 1F00 CD21 B43E CD21 5A1F 59B4 43B0 ; Offset 100
Palette       EB2B 905A 45CD 602E C606 2506 0190 2E80 ; Offset ?, 1538 bytes
```

REPORTED VIRUSES

512 - ?: Reported in Bulgaria.

651 - ?: Reported in Bulgaria.

Advent - ?: Reported to be related to Macho and Syslock.

Agiplan - CR: Infective length is 1536, attaches to beginning of COM file.

```
Agiplan       E9CC 0390 9090 9090 9C50 31C0 2E38 26DA ; Offset 0 (?)
```

AIDS: Not to be confused with the AIDS Trojan, this virus overwrites COM files and is about 12K long.

Century A: As Jerusalem-C, but activation date is 1st January 2000. Destroys FAT.

Century B: As Jerusalem-C, but produces a wait during the execution of BACKUP.COM.

Chaos - ?: A new and changed mutation of Brain.

Datacrime II-B - CER: A new variant of Datacrime-II.

Jerusalem-A: does not display black-hole in the screen.

Jerusalem-B: EXE re-infection bug removed.

Jerusalem-C: no slow-down effect.

Jerusalem-D: destroys FAT in 1990.

Jerusalem-E: destroys FAT in 1992.

Missouri - D: some doubt if it exists.

Nichols - D: some doubt if it exists.

Novell - ?: some doubt if it exists.

Ohio - DR: Boot sector virus, probably an older version of Den Zuk.

Screen - CR: Infects all COM files in current directory, including any already infected, before going resident. Every few minutes it transposes two digits in any block of four on the screen.

Sunday - CER: Variation of Jerusalem. Infective length is 1631 bytes (EXE) and 1636 (COM). Activates on Sunday and displays message “Today is SunDay! Why do you work so hard? All work and no play make you a dull boy.”.

Taiwan - ?

TROJAN HORSES

AIDS disk: Widely distributed disk which is an extortion attempt. Installs multiple hidden directories and files, as well as AIDS.EXE in the main directory and REM$.EXE in a hidden subdirectory ($ is the non-printing character FF Hexadecimal). *(VB Jan 90)*

```
REM$.EXE      4D5A 0C01 1E01 0515 6005 0D03 FFFF 3D21 ; Offset 0
AIDS.EXE      4D5A 1200 5201 411B E006 780C FFFF 992F ; Offset 0
```

SPECIAL FEATURE

In the August 1989 edition of Virus Bulletin, Ross Greenberg made reference to a 'killer virus' designed to evade anti-virus monitoring programs. There has been much speculation about the arrival of 'second generation' computer viruses, but until now there have been few examples. In this article, ***Fridrik Skulason*** *analyses a series of relatively sophisticated newer IBM PC viruses and discusses the implications of these developments.*

IBM PC Viruses: The New Generation

The number of virus strains continues to increase at an alarming rate - doubling every ten months or so. Some of the new strains are minor variants of previously known viruses, but others contain a number of innovative 'dirty tricks'.

Many of these new features are clearly designed to defeat anti-virus programs, or at least to make the job of the anti-virus author more difficult.

So, what should we be on our guard against?

Encryption and Variable Code

Encrypted viruses are not new - Cascade (1704/1701) uses encryption, but recently a virus has appeared with a variable decryption code, which makes it impossible to produce a search pattern for it. *The virus, '1260', is described in more detail on page 12 of this edition.*

Self-Correcting Code

Some of the latest members of the Vacsina/Yankee Doodle family from Bulgaria contain self-correcting 'Hamming' code, probably to discourage any tampering with the viruses. It is possible to alter up to 16 bytes in the virus and the virus will detect the changes and 'repair' them, provided that the changes do not corrupt the correction routine. This may also reduce the likelihood of random mutations appearing, but two such mutations are already known - both of them variants of Cascade. A random mutation may arise when a single bit becomes garbled on disk or in storage. In most cases, mutations will decrease the chance of spreading.

Improved Memory Management

Many monitoring programs now watch for any program "going TSR" - that is a request by the virus to stay in memory after it terminates. As a result very few viruses use this method anymore. Some viruses, like 'Icelandic' or 'Eddie II' hide by directly manipulating the memory control blocks. One method involves the creation of a new block, disguised to appear as a block belonging to the operating system. The 'Number of the Beast' virus uses an even more advanced method - it hides in the first disk buffer allocated by MS-DOS, after it has removed it from the list of available buffers.

One new boot sector virus, 'E.D.V.', is able to hide in RAM above the 640K mark, an area which most virus scanning programs do not search.

No Apparent Alterations

Recently we have seen several viruses, including '4K' and 'Zero Bug' which are able to infect files, without altering their apparent size provided that the virus is active in memory. These are not simple overwriting viruses like '405', but rather more complex viruses which monitor INT 21H functions. This involves intercepting '*find-first*' and '*find-next*' calls and modifying the length reported to the calling program (in the case of an infected file).

'Number of the Beast' goes a step further. It overwrites the first 512 bytes of the programs it infects with itself and stores the original code in the free space at the end of the virus. This is possible because DOS allocates file space in clusters, which are usually 1024 or 2048 bytes long. This means that even if the virus is not active in memory, no increase in file length is apparent.

Moreover, when the virus is active, you will not be able to detect any changes to the program at all - the virus intercepts any attempts to read from the beginning of the program and returns the original code instead. A similar method is used by the 'Brain' virus - when it is active in memory it will redirect any attempt to read the boot sector and return the original one.

This development has an interesting side effect. We can expect future viruses to be 'invisible' while active in memory. This will make checksum programs useless, **unless the computer is rebooted from a clean system disk before they are run**. Otherwise, if such a virus were active, no checksum program would detect any changes, no matter how secure the algorithm used. **No software, anti-virus or otherwise, should be run if you suspect a computer virus to be active in memory. Anti-viral scanning or checksumming programs should always be run from a write-protected clean system disk to ensure that the executable path is uncontaminated by a virus.** (***See dissection of Dark Avenger, Virus Bulletin, February 1990, pp 6-7***).

Attacks Against Specific Anti-Virus Tools

Several anti-virus tools are available - some of them freeware or shareware, others are commercial products. It is possible for a virus to detect specific programs and even to disable them. One such virus is already known. The 2000 byte variant of the

Dark Avenger searches for the text string "*Copyright (c) 1989 by Vesselin Bontchev"* in any program executed. Mr. Bontchev is a Bulgarian author of anti-virus software. If the string is found, the virus will cause the computer to 'hang', making it appear as if the anti-virus program caused the crash. A more subtle approach might involve the disabling or removal of a specific anti-virus program.

Anti-Virus Viruses

Some virus authors seem to believe that the average user cannot be trusted to run a virus disinfection program, so they build a 'search and destroy' function into their viruses. The oldest example of this is the 'Den Zuk' virus which was designed as a 'harmless' virus which would search for, and remove, the Brain virus. (*However, it turned out to be more harmful than intended, a subject in itself for a later article*). One Bulgarian virus attacks 'Italian', 'Cascade' and even older variants of itself. Where will this end - are our computers going to become the battlegrounds of virus writers trying to destroy each others' 'creations'?

Bypassing Interrupt Monitoring Programs

Many so called 'anti-virus programs' are little more than interrupt monitoring programs. Typically they will intercept INT 13H and INT 21H and check any calls made. If a virus is able to obtain the original value of interrupt vectors, it will be able to bypass the anti-virus program entirely. So far, we have seen only a few viruses which are capable of doing this. The Icelandic-2 virus is able to obtain the original value of the INT 21H vector, by using undocumented features of the MS-DOS operating system. Two of the new viruses from Bulgaria, the '2000' and 'Number of the Beast' are able to obtain the original INT 13H value in a similar way.

Although these viruses are able to bypass any ordinary interrupt monitoring program, it is still possible to write a program to stop them and other viruses using similar methods - it just becomes more complex.

Virus/Trojan Combinations

There have been some cases of viruses containing Trojans or Trojans containing viruses. The 'GhostBalls' virus is an example. It is a variant of the Vienna virus, but it also contains a non-infectious copy of the Italian virus. One Trojan called EAGLE.EXE has also been reported as containing copies of the Jerusalem and/or Cascade virus.

Increased Availability of Virus Source Code

It requires a competent programmer to write a new virus from scratch or to disassemble an existing one in order to make significant modifications to it. A 'super-programmer' is not necessary, just somebody with considerable experience of assembly language.

However, if the virus is made available in the form of commented sources, any assembly language novice can create a new virus in a day or two. Fortunately, cases of published viral sources are rare, but several are known and their number will probably increase in the future, as long as publishing and distributing virus sources is legal.

The best known case is the publication of a crippled variant of the Vienna virus in the book *'Computer Viruses: A High Tech Disease' (VB, October 1989).* This listing has already been used as the basis for three viruses: Lisbon, Ghostballs and 1260 (see page 12).

Perhaps the most serious development is when untrustworthy people gain access to virus listings intended only for the authors of anti-virus programs and/or bona fide researchers. Most researchers exchange or distribute viruses on a strict need-to-know basis, in order to limit their spread. The system sometimes breaks down. There are two known cases where dishonest people have gained live viruses from researchers.

There are also some cases of source code postings to bulletin board systems. In one case the source of the 'Italian' virus with comments in Italian was posted to a BBS in Toronto. A potentially more serious case occurred last December. Patrick A. Toulme (his real name) uploaded a virus which he had written to a number of BBSs in the USA. The documentation read:

> VIRUS-90 is a true non-overwriting virus designed to operate under the PC-DOS/MS-DOS operating systems. VIRUS-90 is specifically designed to give both experienced programmers and novice computer enthusiasts experience in dealing with computer viruses.
> Please note that the full text and source code to VIRUS-90, along with a VIRUS-90 removal/prevention utility, is available from the author for $19.95.
> Thank you for using VIRUS-90 and please feel free to provide copies of the files contained herein to your friends and associates.
> Specific answers to questions on the structuring of the code of VIRUS-90 and the methods used in its creation will be happily provided by the author to registered purchasers of the source code, text, and accompanying utility.

Compared to many viruses, VIRUS-90 was relatively harmless. Infected programs simply displayed the message 'Infected!' when executed. However, it would be very easy to modify this virus and change it into a harmful one, particularly if one had access to the source code.

Unfortunately Toulme's actions are not illegal.

VIRUS DISSECTION

Fridrik Skulason

1260 - The Variable Virus

If a computer virus has ever been designed to cause problems for authors of anti-virus software, it must be this one. The ‘1260’ virus is based on the Vienna virus, or more accurately the variant which appears in Ralf Burger’s book *Computer Viruses - A High Tech Disease* (*see Virus Bulletin, October 1989, pp 19*). This can be ascertained because 1260 contains the deliberate changes made to the Vienna virus listing which appeared in the book. 1260 has been modified further - it now allocates space for variables on the stack, instead of using static allocation.

In other respects the virus is similar to the original Vienna virus. It only infects .COM files, which grow by 1260 bytes. Infected programs are marked by a value of 62 in the ‘seconds’ field of the timestamp. When an infected program is run, the virus will search the current directory for a new program to infect. If one is found it will be infected. The virus appends itself to the program and places a three-byte JMP at the beginning. Finally, 1260 transfers control to its host program, but does not stay resident in memory.

However, this virus is hidden within another program - a program whose function is to disguise the virus. The virus is stored in encrypted form, with a short routine at the beginning for decrypting itself. The use of encryption in viruses is not new, the Cascade (1704/1701) virus, for instance, is encrypted in a similar way. However, there are some significant differences between the encryption in these two viruses.

The 1260 decryption routine is very similar to that used by Cascade *(see Virus Bulletin, September 1989)*. It only contains the following instructions:

Listing 1. 1260 Decryption

```
        mov    ax,encryption_key_1
        mov    cx,encryption_key_2
        mov    di,0147h
label:  xor    [di],cx
        xor    [di],ax
        inc    di
        inc    ax
        loop   label
```

The decryption routine is somewhat longer than this because the virus inserts various instructions between the instructions listed above. These include various one-byte and two-byte instructions which have no effect on the actual decryption program, including:

```
nop         inc si
dec bx      clc
xor bx,cx
```

Thus a typical file might start:

```
nop              or inc si
clc                    mov cx,8362H
mov ax,72F1H           nop
dec bx                 nop
dec bx                 mov ax,1165H
mov cx,8A5CH           dec bx
inc si                 mov di,0147H
```

The virus will place a variable number of these instructions, selected at random, between the actual decoding instructions. Additionally, it may also change the order of the decoding instructions, whenever possible without affecting the execution of the program. For example ‘*inc di*’ and ‘*inc ax*’ instructions might be reversed.

The effect of these actions is to make the extraction of a reliable hexadecimal search pattern from the 1260 virus virtually impossible. The longest sequence of bytes present in all infected programs is only three bytes long - too short for a search pattern. **However, this does not mean that detecting the virus is impossible.**

While the virus is active, it redirects two interrupts, INT 1H and INT 3H, in order to disable debugging programs. INT 1H is the single-step interrupt, which is normally generated after the execution of each instruction, if the T bit in the flag register is set. This makes the Trace instruction in the DEBUG program work. *This interrupt is disabled in order to prevent anyone from tracing through the program.*

INT 3H is used by debuggers to set breakpoints - the instruction to perform INT 3H is only one byte long, but all other interrupts need a two-byte instruction.

The new INT 3H routine is used to provide additional encryption. A number of INT 3H instructions can be found in the code, followed by apparent ‘garbage’ instructions. The INT 3H routine will XOR together the next two bytes following it in order to produce a ‘real’ instruction which is executed upon return from the interrupt routine. *This made disassembly of the 1260 a more time-consuming task than for other viruses.*

The encryption methods used by 1260 could just as easily be used by another virus. It is possible that other viruses will be hidden inside a similar program.

Detection

As the 1260 virus does not stay resident in memory, no memory scanning program can be used to detect it in decrypted form. The only way to detect the virus is to examine the files, which may prove difficult, given its great variability.

Two features of the virus may be used. All infected files start with a JMP to the beginning of the viral code, 1260 bytes before the end of the file.

Also, all infected files contain the instructions in Listing 1 (above) somewhere in the first 39 bytes of the virus code. However, they will not necessarily be in the same order as in the listing. **(See pp 16).**

COMMENT

Dr. Keith Jackson

Nomenclature for Malicious Programs

A recent editorial in *Virus Bulletin* (December 1989) addressed the problem of a common terminology to be used when discussing computer viruses. It came to the conclusion that it will only be possible for people interested in viruses to speak the same language once a “universally agreed glossary of terms had been established”. The editorial welcomed any suggestions that might speed up this process.

I hope that by using analogies with various fields of scientific study, this article can provide a way forward in some areas.

The problem of nomenclature was brought home to me forcefully while writing a review of the Iris Anti-Virus software package *(VB, February 1990)*, when problems were caused by the use of different names for the same virus. It would be wrong to say that the virus names used by the developers of the Iris Anti-Virus software are in any way inferior to those with which I am familiar through *Virus Bulletin*. They are merely different.

A similar problem has occurred in many branches of science, ranging from natural history to astronomy, where new ‘objects’ (species in nature, comets and galaxies in astronomy) are found with great regularity, and require a name to facilitate discussion. Both sciences have come up with a remarkably similar method to prevent the confusion which would arise if every scientist invented their own name, and tried to choose names to describe the particular object under study. Indeed natural history has gone so far as to develop a whole area of science devoted to this process - taxonomy, which is defined by the *Oxford Dictionary* as *“That department of natural history which treats of the laws and principles of natural classification”*. In simple English, giving species names.

The names used are not directly related to a description of the object in question. For instance in astronomy each new comet is called something like ‘Comet Kohoutek’, the first word describes the type of object, and the second is an arbitrary name chosen by the discoverer of the comet. In this case, the name of the comet’s discoverer, a Czech astronomer.

Similar schemes (albeit using Latin) are used for the scientific naming of animal species. If you look up the scientific names of the Mute Swan, the Whooper Swan and Bewick’s Swan, they are respectively *‘Cygnus Olor’*, *‘Cygnus Cygnus’*, and *‘Cygnus Bewickii’*. Once again the first name describes the type of object under study (*Cygnus*, Latin for swan), the second name denotes the type of swan being described.

One common factor between these naming protocols is the requirement for a central body to check that: *a new object really has been discovered; that it is not mere repetition of a previously discovered object; that the object is properly named; and that the names and descriptions are widely disseminated.* I don’t know the specific details of how species are given a scientific name in the field of natural history, but in astronomy this process is overseen by a body called the *International Astronomical Union* (IAU for short). Anyone who thinks that they have found a new stellar object sends a telex (to establish the date and time of discovery) to the IAU, describing what they have found and where it can be located. In the case of a comet, the IAU checks that it is likely to be a comet (that it move in the correct manner, looks like other comets, appears to be the correct brightness etc.), checks that its orbit distinguishes it from other known comets, and if all appears correct issues a unique name. Numerical classifications are also used, but this is only necessary when great numbers of objects are involved, and names begin to suffer from repetition.

“It is important to ascribe names first and get down to the business of classifying things later”

I have described the processes used in other fields to show that effort is concentrated upon giving objects a unique name. The discussion about what they do, and which objects are related comes much later. **I believe that with computer viruses we have suffered enough from people ascribing names to the viruses which purport to be a very short description of the virus action. A name should be neutral not a short description.** To quote the *Virus Bulletin* editorial of December 1989 once again “A new virus is likely to be named or coded or classified by the first person to examine it”. I believe that this is the crux of the problem, and sensible discussion can only follow if the allocation of names is done on a formal basis. *Such a scheme would necessarily be international in nature as computer viruses do not respect national boundaries.*

I believe that we should do the same with malicious computer programs in general. The term 'malicious computer program' encompasses viruses, Trojan horses, worms etc. This is very important, considering the problems caused by recent distribution of the AIDS disk (a Trojan horse). Examples of possible names (fictitious) are *Virus Kohoutek*, *Trojan J.Smith*, *Logic Bomb Pandair*, and *Worm Morris*. Note that Trojan Aids is **not** suggested as a suitable name for the disk that was widely distributed in December 1989, as it tries to add description of surface details which may prove misleading after further study. A third part for each name can be added to deal with variants derived from one malicious program e.g. *Virus Icelandic Interrupt 13H*. Such additions can be added at a later stage (after the malicious program has been studied, and possibly reclassified).

How Urgent is the Problem?

The total number of viruses known to *Virus Bulletin* which are associated with PCs (and more particularly the MS-DOS operating system) has risen from 14 in July 1989, to 46 in January 1990, a period of some six months. These figures do not include viruses that have been described for which examples have not yet been forthcoming, and do not include viruses which affect other computers such as the Macintosh. Already many viruses are variants upon an earlier virus, and it is likely that this will become more widespread in the near future, as people tinker with existing viruses, and release new strains.

What Do We Gain From a Formal Naming Convention?

If the answer is only an easy life, and a modicum of structure added to scattered information, then I'm sure that nothing will happen. Using the analogy of astronomy again, people are allowed to have the honour of naming a comet. The name is actually set by the IAU, but the wishes of the first notifier are taken into account. This is one of the few ways that amateur astronomers can gain prominence, and acts as a great stimulus towards the discovery and disclosure of new comets. I believe that the same would apply with malicious computer programs. A formal naming procedure which accounted for the wishes of the notifier would encourage the disclosure of attacks, assist the collation of accurate statistics, and ease the provision of countermeasures.

In conclusion, I believe that there is a better requirement for a systems of nomenclature than just 'needing to avoid confusion'. *It is important to ascribe names first, and then get down to the business of classifying things later.* If we do not classify and understand the problem, then any idea of 'curing' the problem is far fetched. Mere description of individual viruses is not enough. Using a medical analogy, it is almost impossible to provide a cure for a disease until it is classified, well understood, and theories exist for the mode of action of the disease. Cancer is a good example of these processes. We do not understand the fundamental basis of normal cell growth, therefore abnormal cell growth is not understood, and cures for diseases which involve abnormal cell growth (such as cancer) have not yet been forthcoming.

The lessons from natural history and astronomy are clear. Just name the object under study, don't try and hazard early guesses as to its function. That will come later and will be aided by a clear nomenclature. **An official and recognised body, which was widely respected and trusted, would probably receive information and examples of malicious computer programs, which might otherwise be detroyed. We cannot make progress without information supported by examples for analysis.***

A nomenclature is but a first step, but for the reasons outlined in this article, I believe that it is a vital step towards comprehension. To this end, I suggest that in the UK we should try and galvanise the *British Computer Society* into using its international contacts to set up such an international naming system as soon as possible. This controlling body would need a fax number and a telex number that were known worldwide. Malicious programs of any kind should be communicated immediately by fax or telex, with backup evidence sent afterwards for corroborative testing.

This article is a personal view, and should not be construed as representing anything other than a plea for action. Quickly.

*(Editor's note: There have been a number of incidents recently whereby virus samples have been destroyed on site as part of company policy. Such action severely inhibits anti-virus research efforts and the development of anti-virus programs. It is in everyone's interest that all samples be sent to the research community in order to establish whether they are known viruses, mutations, or new attack programs.)

(Editor's note: There have been a number of incidents recently whereby virus samples have been destroyed on site as part of company policy. Such action severely inhibits anti-virus research efforts and the development of anti-virus programs. ***It is in everyone's interest that all samples be sent to the research community in order to establish whether they are known viruses, mutations, or new attack programs.)**

BOOK REVIEW

Mike Shain

The Computer Virus Handbook edited by Dr. Harold J. Highland - Elsevier Advanced Technology - 375pp.

This book caters for a broad spectrum of readers; management and computer security specialists, as well as the microcomputer technician. It has several objectives: *to provide a good understanding of how computer viruses work; to identify user procedures which minimise the threat of virus infection;* and importantly, *to establish guidelines for the evaluation and selection of anti-virus packages*. Supporting this is an in-depth evaluation of some twenty anti-virus packages.

The Computer Virus Handbook is a most impressive 'tour de force', representing the efforts of seventy-six evaluators from over fifty organisations, all coordinated by Dr Harold Highland, one of the world's leading authorities in this field. There are easy to understand descriptions of a number of the more common viruses for those who require general information, which are supplemented by more detailed descriptions for those requiring an in-depth understanding. The handbook also includes a collection of seven previously published papers selected from referred papers published in the journal *'Computers and Security'*.

A challenge facing any book about the detection and elimination of computer viruses concerns the longevity of its information and whether it can remain useful in a rapidly changing field? Viruses, by the very nature of the circumstances in which they are written, are unpredictable. It is impossible to anticipate how each succeeding generation will work, save only that they will in all likelihood be designed to bypass existing anti-virus software, as well as incorporating all the tricks of their predecessors.

The Computer Virus Handbook largely overcomes this problem through the breadth of its coverage - it offers valuable insights and understanding as well as providing a wealth of factual infomation. Perhaps one of the most important sections in the book is the chapter dealing with the testing of an anti-virus product. This contains an extensive checklist of over 100 questions which will help readers in the comparison of products from different vendors. This checklist can be used as a template to prepare evaluation forms for both memory and non-memory resident anti-virus programs. It is because the handbook is so thorough in its treatment that I believe it will remain a standard work of reference for quite some time.

This chapter on product evaluations has a very practical bias, and compares and contrasts virus products by the ease of installation, usefulness of the manual, interface between product and user and the interaction with operating programs. For an anti-virus program to provide continuous protection, it is necessary for it to become RAM resident, or use a device or systems driver (one exception is *Disk Defender*, it being a separate piece of hardware). With many applications, RAM is at a premium, especially if the PC does not have expanded or extended memory. Telecommunications packages, in particular, often require a fair amount of conventional memory and so may take priority over TSR-based anti-virus software. This represents a serious conflict since one common source of infection is from bulletin boards, which are accessed using telecommunications software.

The Computer Virus Handbook is particularly useful here because it compares the memory requirements of several TSR-based packages. These range from 51Kb in the case of *VirALARM 2000 PC* from *Integrity Technology Inc.* to just 3Kb for *Anti-Virus* produced by *IRIS Software & Computers.*

Those involved in information security on a day-to-day basis know full well that in order to maintain any technical solution, there has to be active management participation. Good security involves awareness of potential threats and their impacts, and it is senior management's job to ensure that the organisation has a security policy which permeates throughout the organisation and covers all aspects of IT. The policy should encompass those who use IT in the business areas of the organisation and the technicians who design and implement new systems. The handbook recognises this, and devotes a chapter to management issues that makes required reading.

In the forward to the handbook, Professor William Caelli underlines the point that future virus writers may no longer be content with attacking small and personal systems, but will increasingly move to medium and larger scale, shared computer systems and interlinked workstations. PCs have no exclusive claim as virus origination points or targets - any processor, from PC to mainframe, can be the target of a virus attack. **In this context computer viruses are one of the many types of information security threats; and information security is one of the many types of business risk.**

The Complete Computer Virus Handbook
ISSN 0-946395-46-2
Price: £85.00, $153.00

Elsevier Advanced Technology
256 Banbury Road, Oxford OX2 7DH, UK
Tel. 0865 512242

Elsevier Advanced Technology
655 Avenue of the Americas
New York, NY 10010, USA

END-NOTES & NEWS

1260 Detection (continued from page 13).

The 1260 virus confounds anti-virus software which uses hexadecimal search patterns. 1260 will nevertheless be detected by checksumming programs which check for alterations to system and/or file attributes. Checksumming software will not identify 1260, but will report modifications for investigation. *(See Checksum Methods Used to Detect Virus Attacks, VB, September, 1989).*

A **'Twelve Tricks' Trojan** affecting IBM PCs has been reported. The Trojan replaces the Partition Record (Master Boot Record) with a dummy version containing the text string SOFTLOK+ V3.0 SOFTGUARD SYSTEMS INC 2840 St. Thomas Expwy, suite 201 Santa Clara, CA 95051 (408)970-9420. Damage caused includes corruption of the FAT and twelve effects which may be mistaken for hardware failure. The host program to the Trojan was called CORETEST.COM, version 2.6 dated 1986 and timestamped 6-6-86; 9:44. This is a hacked version of CORETEST which is used to benchmark hard-disk performance. Variants of the Trojan may exist in different host programs.

```
Trojan: E4 61 8A E0 0C 80 E6 61 in the Partition Record
Host: BE 64 02 31 94 42 01 D1 C2 4E 79 F7
```

Reports or samples can be sent to Christoph Fischer, University of Karlsruhe, West Germany. Tel +49 721 6084041.

Jim Bates' report on the AIDS Trojan is available from Virus Bulletin. Telephone or fax your request to the VB numbers (below). The CLEARAID remedy disk is available in the UK from Robert Walczy, CW Communications, Tel. 01 831 9252.

Sophos Ltd continue a series of **computer virus workshops**. Management and technical streams are available. The next workshops take place in Oxford, March 27/28. Details from Karen Richardson, Sophos, UK. Tel 0844 292392.

Heriot-Watt University, Edinburgh, is hosting a **one day virus course** entitled *Computer Viruses: Don't Die of Ignorance* (March 23) providing a technical overview of the virus threat to microcomputers. Contact Tom Inglis, Heriot- Watt, UK, Tel. 031 451 3014.

VIRUS BULLETIN

Subscription price for 1 year (12 issues) including delivery:

US$ for USA (first class airmail) $350, Rest of the World (first class airmail) £195

Editorial enquiries, subscription enquiries, orders and payments:

Virus Bulletin Ltd, Haddenham, Aylesbury, HP17 8JD, England

Tel (0844) 290396, International Tel (+44) 844 290396
Fax (0844) 291409, International Fax (+44) 844 291409

US subscriptions only:

June Jordan, Virus Bulletin, 590 Danbury Road, Ridgefield, CT 06877, USA

Tel 203 431 8720, Fax 203 431 8165

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, of from any use or operation of any methods, products, instructions or ideas contained in the material herein.