SPECIAL FEATURE

Dr. Jan Hruska

Virus Writer and Distributors

'Attributable Viruses'

It is not easy to establish the origins of a computer virus and it is rare that positive indicators as to authorship can be found by examining virus code. There are, of course, notable exceptions to this.

The Brain virus, for instance, includes the authors' names, address and telephone numbers embedded in the boot sector. The virus code was written by two computer software retailers and was reportedly developed as a means of copy-protection - a measure to punish 'bootleggers'. (see *Figure 1*.)

Toulme

Patrick A Toulme of the United States is a high profile virus writer. Earlier this year he uploaded his 'Virus-90' to a number of Bulletin Boards in the United States ad requested a fee of $19.95 (see *VB, March 1990*). His latest release is 'Virus-101', an 'improved' version of his earlier creation. Virus-101 is a memory resident self-modifying and encrypting virus which makes the extraction of reliable hexadecimal pattern virtually impossible. Fridrik Skulason reports that patterns to search for the virus may be possible with the use of 'wild card' characters in the hexadecimal pattern although the virus is still under examination. Virus-101 will probably necessitate the use of a 'virus identity' to identify infected files (see '1260 Revisited', *VB, April 1990*).

Toulme claims that these viruses are *"designed to give both experienced programmers and novice computer enthusiasts experience in dealing with computer viruses".* There seems little legal redress against such activities, although an infection caused by Virus-90 or -1`01 on US federal interest computers might expose him to prosecution under the *US Computer Fraud and Abuse Act 1986.* It is probable that both viruses (and variants of them) will appear in the wild.

Virus-B

The development of 'Virus-B' by John McAfee's *InterPath corporation,* USA is another example of an 'attributable virus'.

Virus-B is not, in fact an entirely new specimen, but a modified version of the South African virus (which InterPath call X-12). Virus-B only infects .COM files and displays a clear infection message upon execution of infected programs. According to the documentation the virus will:

> *"...increase the size of the infected program by about 500 bytes. An infected program will cause no damage but it will be a nuisance if a large number of system's programs become infected."*

The documentation also acknowledges certain dangers including the possibility that *"Hackers could re-activate Virus-B to return to destructive mode".* It goes on to say that *"Such a person could just as easily write a virus from scratch if they were so inclined, but the potential for reactivation exists."*

Reference is made to 'built in protection mechanisms' which explains that the code segment for the destructive mechanism has been left intact ("*so that it may be analysed*") but that the branch instructions to these segments have been removed. A dire warning follows: *"DO NOT ATTEMPT TO DISASSEMBLE THIS VIRUS AND RECONNECT THE BRANCH INSTRUCTIONS".*

Virus-B was made available by InterPath as a 'restricted' access file' and was *"developed to be used in a research environment for studying virus replication activities and as a safe tool for testing anti virus measures".*

Problems abound with 'demonstration and 'test' viruses and one can only hope that *InterPath Corporation* exercised proper judgement in the people to whom it distributed Virus-B.

Burger and Morris

The case of Ralf Burger his 'VIRDEM' demonstration virus is discussed by Jim Bates on page 6 of this month's VB. It would appear that Burger distributed a number of different virus demonstration disks, some of which have now appeared in the wild. Burger's primary motivation appears to be financial gain from the virus phenomenon.

VB has, over the months, also covered the case of Robert Morris and the Internet worm program. Morris is the first man convicted under the aforementioned *US Computer Fraud & Abuse Act.* Intellectual challenge seemed to have been the motivating force behind the development and release of the program. This is not surprising from a computer science graduate at one of the principal US universities - Cornell.

The Bulgarians

Lubomir Mateev Mateev and Iani Lubomirov Brankov wrote and distributed the Murphy virus in Bulgaria - they included their telephone numbers and addresses in the source code which they circulated. No prosecution will result within Bulgaria which, like so many countries, has no applicable legislative power.

Sofia is home to a dedicated group of virus writers including 'T.P.' and Dark Avenger'. The writers of the Bulgarian viruses are almost certainly students from a research institute attached to the *Bulgarian Academy of Sciences* or from a faculty at *Sofia University* or the *'Lenin-V.I.' Higher Institute of Mechanical and Electrical Engineering.*

Apart from these rare examples, computer virus writers generally choose anonymity, although careful study of text strings and programming style can reveal details about the programmer's age, nationality and personality.

Other Possible Sources

Various motivations lie behind the development of the attributable computer viruses mentioned above. It is quite useful to speculate on other possible groups or individuals involved in virus writing and distribution.

A number of groups are readily identifiable as potential (high likelihood) originators of computer viruses.

Hackers and 'Technopaths'

In the book *Out of the Inner Circle,* the author Bill Landreth describes the various motivations behind computer hacking. He describes five hacker sub-classes - novice, *student, tourist, crasher* and *thief.* Of these sub-groups he identifies two categories as liable to inflict damage to computer systems. The 'novice' often causes damage unintentionally due to inexperience and carelessness but is also prone to vandalism. However, Landreth singles out the 'crasher' as

> *"a troublemaker motivated by the same elusive goals as a vandal. If it weren't for computers, her could just as easily be spray painting his name on the side of a building, or perhaps, even setting the building on fire".*

The author asserts that genuine hackers aspire to either 'student' or 'tourist' class and hate 'crashers' because the give hackers a bad name, they close accounts which hackers have spent time and effort to obtain and they crash bulletin board systems on which hackers communicate. The behaviour as described would be clinically defined as psychopathic. The computer world has adopted the term '*technopath*' to describe this type of personality disorder.

The willingness to inflict damage to computer systems makes the 'crasher' a potential computer virus writer.

```
000000  fa e9 4a 01 34 12 00 09  22 00 01 00 00 00 00 20  ..J.4... ``......
000010  20 20 20 20 02 20 57 65  6c 63 6f 6d 65 29 74 6f        We lcome to
000020  20 74 68 65 20 44 75 6e  67 65 6f 6e 20 20 20 20   the Dun geon
000030  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
000040  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
000050  20 28 63 29 20 31 39 38  36 20 42 61 73 69 74 20  (c) 198 6 Basit
000060  26 20 41 6d 6a 61 64 20  28 70 76 74 29 20 4c 74  & Amjad (pvt) Lt
000070  64 2e 20 20 20 20 20 20  20 20 20 20 20 20 20 20  d.
000080  20 42 52 41 49 4e 20 43  4g 4d 50 55 54 45 52 20   BRAIN C OMPUTER
000090  53 45 52 56 49 43 45 53  2e 2e 36 33 30 20 4e 49  SERVICES ..730 NI
0000a0  5a 41 4d 20 42 4c 4f 43  4b 20 41 4c 4c 41 4d 41  ZAM BLOC K ALLAMA
0000b0  20 49 51 42 41 4c 20 54  4f 57 4e 20 20 20 20 20   IQBAL T OWN
0000c0  20 20 20 20 20 20 20 20  20 20 20 4c 41 48 4f 52              LAHOR
0000d0  45 2d 50 41 4b 49 53 54  41 4e 2e 2e 50 48 f4 4e  E-PAKIST  AN..PHON
0000e0  45 20 3a 34 33 30 37 39  31 2c 34 34 33 32 34 38  E  :43079 1,443248
0000f0  2c 32 38 30 35 33 30 2e  20 20 20 20 20 20 20 20  ,280530.
000100  20 20 42 65 77 61 72 65  20 6f 66 20 74 68 69 73    Beware  of this
000220  20 56 49 52 55 53 2e 2e  2e 2e 2e 43 6f 6e 74 61  VIRUS.. ...Conta
000120  63 74 20 75 73 20 66 6f  72 20 76 61 63 63 69 6e  ct us fo r vaccin
000130  61 74 69 6f 6e 2e 2e 2e  2e 2e 2e 2e 2e 2e 2e 2e  ation... ........
000140  2e 2e 2e 2e 20 24 34 40  25 24 40 21 21 20 8c c8  .... $#@  %$@!! ..
000150  8e d8 8e d0 bc 00 f0 fb  a0 67 7c a2 09 7c 8b 0e  ........  ..|..|..
000160  07 7c 89 0e 0a 7c e8 57  00 b9 05 00 bb 00 7e e8  .|...|.W ......~.
```

Figure 1.

The Brain virus was first reported after infecting floppy disks at the University of Delaware, USA, in October 1987. It has the distinction as being the first virus to strike world wide outside of a laboratory.

It is rare that it is in 'attributable virus' - its boot sector contains the Names of its originators along with their address in Pakistan. Today's virus writers generally choose anonymity.

Students

Most universities offer free, often uncontrolled, computer facilities to students (and often ex-students and even non-students). The conditions for both virus propagation and development are ideal. Illegal software copying is widespread, and virus attacks are continuously occurring at academic institutions.

The appearance of a virus at *Lehigh University* in 1987 (the Lehigh virus) which never infected any other sites indicates that the virus was developed on campus. There is also strong evidence to suggest that the Jerusalem virus was developed by a student or students at the *Hebrew University of Jerusalem*. The Italian virus is believed to have originated at the *Polytechnic of Turin.* The technical ability to write a virus is within the reach of first-year computer science student and, as in the case of Morris at *Cornell,* the primary motivation will be intellectual challenge.

This group are also a potential source of mini and mainframe viruses and worms. Whereas most members of the public can afford a cheap PC, they cannot easily gain access to an IBM 370 or a DEV VAX. The Internet worm is not the only example of this; the CHRISTMA EXEC 'Christmas tree' worm (VB, April 1990) originated at the *University of Clausthal Zellerfield*, West Germany.

Disgruntled Employees and Ex-Employees

Most organisations are acutely aware of the threat posed by this group. Although a computer literate employee might program a 'site-specific' virus, it is more likely that he/she would implant an existing destructive virus or add a destructive segment to a 'benign' (or demonstration) virus. Readiness to cause damage by programming has already been shown in cases of logic bombs being planted in computer systems by disgruntled employees.

Computer viruses, or the threat of unleashing such programs, could also be used during an industrial dispute as part of 'electronic picketing' or 'negotiation'.

Computer Clubs

In 1989 the *Chaos Computer Club* in Hamburg, Germany, devoted an entire private congress to the subject of computer viruses. Chaos have also released a 'Virus Construction Set' for the Atari ST and a diskette containing 'nightmare software'. A Chaos spokesman when asked what motivated the virus writer answered "You feel something wonderful has happened. *You have created something which lives. You don't know where it will go what it will do, and how it will live on".*

Other clubs have a history of creating viruses. The *Swiss Crackers Association* (SCA) released a virus for the Amiga which displays:

```
Something Wonderful has happened. Your Amiga is
alive...
```

Terrorist, Criminals and Politically Motivated Groups

There is no evidence, so far, that terrorist organisations have been involved in writing or disseminating computer viruses. However, the Italian *Red Brigade's* manifesto specifically includes destruction of computer systems as an objective, which should be done by means other than explosive or arson. In France, there is even an underground organisation dedicated to destroying information systems - CLODO - '*the committee to liquidate or neutralise computers'.*

The Jerusalem virus was reported in the *New York Times* as being written "as a weapon of political protest", but several researchers (including Yisrael Tadai of the *Hebrew University* who is the recognised authority on the Israeli Viruses) dispute this. The evidence to support this theory was that the original trigger date of the virus - May 13th 1988 - was the fortieth anniversary of the last day the Palestine had existed under British mandate. This virus is still referred to as the 'PLO' virus.

Computer viruses developed by terrorists and organised crime syndicates will probably make an appearance once their destructive capacity is realised and, significantly, once their potential as tools to commit fraud becomes more obvious. Computer viruses are an ideal way to cause disruption in order to conceal computer fraud. Rumours persist that the original Datacrime virus had been developed and circulated for criminal or terrorist purposes. It certainly caused a national panic among Dutch computer users in October of last year.

Future extortion bids, probably more targeted than that attempted by the '*PC Cyborg Corporation*' with their AIDS Information Diskette (*VB, January 1990*), will increasingly use destructive computer programs.

An underlying political motivation can be discerned in the on-screen messages of certain viruses - notably the Dukakis and Peace viruses on the Macintosh, and the Fu Manchu and New Zealand viruses on the PC.

More significantly, last year's threats involving the unleashing of computer viruses at poll tax offices in Scotland demonstrate an increasing awareness of the potential of these programs as political weapons.