November 1991 ISSN 0956-9979

VIRUS BULLETIN

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

Editor: **Edward Wilding**

Technical Editor: **Fridrik Skulason**

CONTENTS

EDITORIAL

A Little Knowledge is a Dangerous Thing

'*Give a child a hammer and all of a sudden things around him will start looking like nails*.' (Anon.)

No MIS or DP manager in his right mind would hand out *The Norton Utilities* to all PC users regardless of their need or ability to use such powerful and potentially destructive software. The misuse of *Norton* (or *PC Tools* or any other powerful disk editor) could cause untold damage if its distribution were not limited to technically competent staff.

Neither would it be wise to instruct general users as to the existence or nature of certain of the more dangerous DOS commands - most PC users in business run a limited set of applications (text editors, spreadsheets, databases and DTP being prevalent) and can remain happily oblivious to such two-edged swords as *FORMAT* and *FDISK*. Even the humble delete command dons a perplexing mantle when combined with those cheeky wildcard characters '*.*'! Obviously, all of the DOS commands are thoroughly outlined in the user manual - be it from *Microsoft* or *IBM* or *Digital Research*. It is fortuitous in this instance, therefore, that people rarely, if ever, refer to manuals while using software - this is one of the major reasons why software developers employ 'walk-thru' menus. The information and resources to cause untold accidental damage are readily available within DOS itself but are not clearly signposted as such.

The point here is that handing out powerful security and audit tools to the masses, and providing superficial education about the operating system to people who don't need that information, is a recipe for disaster. Instructions to use security tools and techniques should be on a 'need to know' basis - PC Support should know the exact locations of all such software and its distribution should be extremely limited.

In the case of anti-virus software, many packages aim to provide comprehensive virus detection and removal facilities. 'Toolkit' utilities of this sort provide programs to replace boot sectors, edit specific areas of disk and even write protect drives. Is it wise to place such power in the hands of users? Even a simple scanner becomes a complex beast when you examine the number of menu driven or command line options that many developers have provided. Can PC Support be sure that users will comply with their *ex-cathedra* statement to boot from a write-protected system floppy disk? Do users know *what* such a disk is, or *why* they should use it, or *how* to prepare it? Do they even know the difference between drive A: and drive C:?

It is sometimes difficult for technicians to appreciate the relative ignorance of non-technicians - many developers of security software still believe that mass populations can be trained to use their products correctly and effectively. More seasoned and forward-thinking observers knew a long time ago that this belief was nothing more than a pipe dream. Given that it takes a massive and concerted effort to educate users in the most *basic* aspects of corporate security, training a mass community in the use of relatively complex software security packages is a wholly untenable objective.

Security managers in many organisations rightly conclude that they are simply not prepared to trust end-users with *any* degree of technical responsibility when it comes to combating computer viruses. As a result, the tools and techniques for this job are restricted to those capable of using them. This is an *elitist* rather than *populist* approach - considering the wealth of accumulated ignorance in any society it is entirely understandable and well conceived. This is not to belittle education; if a problem can be explained in simple, straightforward and readily understood terms then that is all to the good. However, there is an enormous divide between understanding the basic tenets of a problem and proficiency in dealing with it!

The strategy which is most effective and which has been widely adopted combines three elements: *central reporting*; *specialist response teams* (variously known as PC SWAT or CERT, or simply PC Support) and *risk analysis*. *Central reporting* effectively channels all enquiries and problems to the SWAT team - qualified technicians who have studied the virus problem and who are supplied with the requisite information and tools to deal with any outbreak both swiftly and correctly. *Risk analysis* is the process of identifying the 'mission critical' machines within the organisation. These are the machines from which any loss of availability or integrity would have a serious impact on the overall performance of the organisation. A risk analysis of any organisation usually shows that 'mission critical' PCs comprise a relatively small percentage of overall IT resources. It is vital, however, that these PCs are adequately protected and this *may* necessitate the purchase of suitable defensive software.

One questionable strategy is that of equipping *every* single PC with defensive software. This may be necessary in high security environments but imposes burdens in terms of financial outlay, support costs and inconvenience. Memory-resident software may well cause memory clashes (with *Windows 3.0* or SHARE.COM for example), false alarms and is critically dependent on *user-compliance*. Checksumming software needs careful implementation and management - particularly in an a shifting software environment. Memory-resident software is prone to subversion by stealth viruses as is checksumming software if it is run in an infected DOS environment. Monitors and checksummers can be administered - but not on 5,000 PCs in 60 or 70 locations!

Ultimately, put the diagnostic tools in *capable hands* and purchase defensive software on the basis of considered *risk analysis*. Finally, make friends with *Symantec* and the *Federation Against Software Theft*...locate all unauthorised copies of *The Norton Utilities* and delete them!

VIRUS BULLETIN ©1991 **Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50**

TECHNICAL NOTES

Norton and The Cascade Message

In recent months *VB* and various anti-virus software manufacturers have received a number of calls concerning reports of 'Cascade' by the *System Information* (SI) program supplied with *Norton Utilities* version 5.0. These spurious reports have nothing to do with the Cascade virus and do not imply infection by any virus.

The confusing message is displayed by SI in its list of hardware interrupts, as a description of IRQ2 and refers to the internal hardware of the PC.

PC-ATs contain two 8259A hardware interrupt controller chips, each of which support eight system interrupts. The 8086 family of microprocessors has a single line to communicate with the interrupt controllers, so IRQ2 on the first interrupt controller accepts interrupt requests from the second controller. Thus the two controller chips are connected in a cascading manner - hence the 'Cascade' message.

The actual Cascade virus has been the cause of various misinterpretations; the virus is also known as 1701 which also happens to be a standard disk read error message! Perhaps Hailstorm, Fall, Autumn Leaves or one of the many other aliases for this virus should be adopted and standardised.

FDISK /MBR

Kevin Powis of *Visionsoft* has brought a little known and very useful feature of *FDISK* supplied with MS-DOS 5 to our attention. This feature will effectively remove many current viruses which infect the Master Boot Sector (Track 0, Head 0, Sector 1).

If a PC running MS-DOS 5 is infected by such a virus, the user can boot from a clean write-protected system diskette upon which is stored a copy of *FDISK*.

The *FDISK* program should then be run from the diskette drive. By typing FDISK /MBR at the A: prompt, clean Master Boot Sector code is written to the first physical sector on the hard disk. Moreover, when this *FDISK* option is invoked, all initialisation data in the 64 byte Partition Table stored in physical sector 1 is left completely intact.

Note: this option should only be used if the Partition Table in the first physical sector on the hard disk is present and correct after the Master Boot Sector has become infected. This may not necessarily be the case with future computer viruses. [*Such viruses may already exist. Tech Ed.*]

Fortunately, most viruses which currently infect the Master Boot Sector do not tamper with the Partition Table.

This feature, combined with the ability of *SYS* to remove DOS Boot Sector viruses (those which infect the boot sector of the active DOS partition), provides users of MS-DOS 5.00 with simple standard tools to remove most boot sector viruses without having to resort to formatting. This *FDISK* option is only available under MS-DOS version 5 - it does not apply to versions prior to 5.

It is still recommended that all PC users store clean write-protected backups of the boot sectors of their fixed disks on diskette.

Non-Compliance

Many resident scanners, monitors and standalone checksumming programs provide the option for PC administrators to customise the screen message which appears when these programs detect virus activity. System administrators can thus instruct the user to contact the relevant PC Support desk and provide other information consistent with company policy.

Unfortunately, a user of unauthorised or stolen software, upon seeing a virus alert reported on his screen may decide not to report the incident to PC Support, particularly so if company policy entails severe disciplinary action for illicit software use. Subsequently such a user may attempt to disinfect his machine which may result in compounded damage.

The problem of the non-compliant user is an extremely difficult one to solve. At the recent *Sysguard 91* conference in London, Noel Bonczoscek of the *Computer Crimes Unit* suggested that developers of memory-resident software might consider incorporating a completely customised alert banner into their monitors - upon detecting a virus the on-screen alert could thus be configured in such a way as not to arouse the suspicions of the 'untrusted user'.

This is an interesting suggestion which merits consideration.

Using *Virus Guard* (from *Dr. Solomon's Anti-Virus Toolkit*) as a representative example, this resident monitor, upon detecting a virus, currently flashes a message to screen which states prominently:

```
                      Virus Alarm

   Dr. Solomon's Anti-Virus Toolkit has Intercepted a
                         virus:

  Close everything down normally, then consult Toolkit
                    manual for remedy
```

However, Bonczoscek said that PC administrators might prefer to configure a more subtle display along the lines of 'Internal Error: Do Not Proceed, Contact PC Support/ Tel Extension 203'.

This banner would have no reference to a suspected virus attack or the anti-virus software that had detected such activity but would be sufficient to ensure that the more naive user contacted the appropriate support staff.

This is only one suggested (and, to our knowledge, untested) proposal to encourage user-compliance. The potential pitfalls of such a tactic are readily apparent - not least the fact that a genuine operating system error would not direct the user to an 'in house' telephone extension! Any user recognising this fact might well be capable of dealing with a virus attack in the first place!

However, Bonczoszek's underlying point is that computer administrators should never *assume* that users will automatically comply with company policy and report virus outbreaks or other incidents. (To quote Thomas Harris: 'Never assume anything - you'll make an *ASS* out of *U* and *ME*'). Compliance auditing is one of the most complex tasks in computer security - making sure that people understand the rules and that they are following them is a formidable task and technical solutions do not lend themselves easily to it.

Little wonder that the wisest and most experienced computer security managers don't allow users anywhere near detection and diagnostic software - they know that either it will not be used, or that it will be used incorrectly (often with dire results), or that alerts and warnings will simply be ignored!

Rage Change

An amended scan string to detect the Rage virus (*VB*, October 1991, p. 21) has been supplied by Andrew Busey of *Microcom Software Division Inc*. The scan string contains no addresses and should be used in preference to either of the previously published patterns.

```
Rage B9FD 018A 2451 8AC8 D2C4 5988 24FE C046
```

Nobbled Nibble

A one-nibble error in the search pattern published for the Liberty virus in last month's *VB* effectively invalidated the string. An amended and corrected pattern appears below.

```
Liberty    B931 2833 D2CD 1306 BB5C 0653 CB2E
           803E BCO6 0A74 4633 C08E
```

Anti-virus software developers should take note that the original pattern for this virus (last published in July 1991) should be maintained as essential scan data. This pattern was extracted from an earlier version of the virus which is not consistently detected by the pattern above. The pattern is repeated here:

```
Liberty    0174 031F 595B 5053 5152 1E06 1E0E
           1FE8
```

VIRUS BULLETIN

EDUCATION, TRAINING AND AWARENESS PRESENTATIONS

Education, training and awareness are essential as part of an integrated campaign to minimise the threat of computer viruses and Trojan horses

Virus Bulletin has prepared a presentation designed to inform users and/or line management about this threat and the measures necessary to minimise it. The standard presentation consists of a ninety minute lecture supported by 35mm slides, followed by a question and answer session.

Throughout the presentation, technical jargon is kept to a minimum and key concepts are explained in accurate but easily understood language. However, a familiarity with basic MS-DOS functions is assumed. The presentation can be tailored to comply with individual company requirements and ranges from a basic introduction to the subject (suitable for relatively inexperienced users) to a more detailed examination of technical developments and available countermeasures (suitable for MIS departments).

The aim of the basic course is to increase user awareness about computer viruses and other malicious software without inducing counterproductive 'paranoia'. The threat is explained in comprehensible terms and straightforward, proven and easily-implemented countermeasures are demonstrated. An advanced course, aimed at line management and DP staff, outlines various procedural and software approaches to virus prevention, detection and recovery.

The presentations, are offered free of charge except for reimbursement of travel and any accommodation expenses incurred. Information is available from the editor, *Virus Bulletin*, UK. Tel 0235 555139.

KNOWN IBM PC VIRUSES (UPDATE)

Updates and amendments to the *Virus Bulletin Table of Known IBM PC Viruses* as of 20th October 1991. Hexadecimal patterns may be used to detect the presence of the virus with a disk utility program, or preferably a dedicated virus scanner.

Type Codes

C = COM files E = EXE files **D** = Infects DOS Boot Sector (logical sector 0 on disk)
M = Infects Master Boot Sector (Track 0, Head 0, Sector 1) **N** = Not memory-resident after infection
R = Memory-resident after infection P = Companion virus **L** = Link virus

864 - CN: This virus adds 864 bytes in front of the files it infects. Awaiting analysis.

```
864            B04D B449 B742 473A 2575 153A 7D01 7510 3A45 0275 0BC6 4502
```

1876 - CER: This 1876-byte virus is probably of Polish origin. Awaiting analysis.

```
1876           8EC0 33FF 33C0 B9FF 7FFC F2AE 26F6 05FF 75F8 83C7 038B D72E
```

Best Wishes-970 - CER: This virus is detected by the search pattern for the Attention virus, but not by the pattern for the Best Wishes-1024 virus. This variant is not able to infect .EXE files properly.

Black Wizard - EN: A variant of the 'Old Yankee' virus and detected by the pattern for that virus. This variant is 2051 bytes long and plays a different tune than the original virus, but is otherwise similar.

Bulgarian 123 - CN: A simple 123-byte virus from Bulgaria, which does nothing but replicate. It may infect the same file repeatedly.

```
Bulgarian 123  B103 8D54 F4B4 40CD 21B4 3ECD 21B4 4FCD 2173 AFBB 0001 FFE3
```

Copmpl - CER. This is a 1111 (COM) or 1114 (EXE) byte Polish variant of the Akuku virus. The name is derived from the following text, which can be found inside the virus 'Sorry, I'm copmpletly dead' (sic). The only effect of the virus is to play a tune.

```
Copmpl         80E6 0F8A D680 FA00 7407 80FA 0B76 06B2 02B4 0ECD 218C C88E
```

Copyright - CN: A 1193-byte virus from East Europe, which contains a fake Award BIOS copyright message. Awaiting analysis.

```
Copyright      AB4A 75F2 E2EA 33C0 CD16 B800 06B7 0733 C9B6 18B2 4FCD 10E9
```

DIR-II - LCER: A 1024-byte 'link' virus from Bulgaria. 'Infects' all COM and EXE files in each directory on a single pass. If the virus is resident, 'infected' COM and EXE files can be disinfected by renaming their extensions. (*VB*, Nov 1991).

```
DIR II         BC00 06FF 06EB 0431 C98E D9C5 06C1 0005 2100 1E50 B430 E824
```

DM-400 - CR: This 400-byte virus does not seem to do anything but replicate. It contains the text '(C)1990 DM'.

```
DM-400         80FC 4B74 3380 FC56 7419 FE04 80FC 3D74 12FE 0480 FC3E 751C
```

Europe '92 - CR: This 421-byte virus activates if the year is set to 1992, when it displays the message: 'Europe/92 4EVER!'

```
Europe '92     B450 CD21 8CD8 488E D8C6 0600 005A 891E 0100 8916 0300 53B8
```

Fake-VirX - CN: A 233-byte virus from Finland which activates on any Friday the 13th, when it displays the message 'VirX 3/90'.

```
Fake-VirX      408B D5B9 0600 CD21 B801 575A 59CD 21B4 3ECD 21B8 0001 FFE0
```

Gergana - CN: Four variants of the Gergana virus, which are longer than the original with improved error handling.

```
Gergana-222    BF80 FFB9 3000 F3A4 E9C6 FD5E 81C6 0001 BF00 01B9 DE00 F3A4
Gergana-300    BF80 FFB9 3000 F3A4 E985 FD5E 81C6 0001 BF00 01B9 2C01 F3A4
Gergana-450    BF80 FFB9 3000 F3A4 E97E FD5E 81C6 0001 BF00 01B9 C201 F3A4
Gergana-512    BA00 FAB4 3FCD 21C3 B900 02B4 40CD 21C3 B801 572E 8B0E 5001
```

Gosia - CR: A 466-byte virus from Poland. It contains the text 'I ♥ Gosia'. ♥ is the ASCII character (03))

```
Gosia          0275 10AC 268A 2547 3AC4 7405 80CC 203A C4E2 EE9F 03F9 8B1D
```

Gotcha - CER: Two related viruses from East Europe, 879 and 881 bytes long. They contain the text string: 'GOTCHA!'.

```
Gotcha         9C3D DADA 7428 80FC 3D74 0A3D 006C 7405 80FC 4B75 1306 1E50
```

Hero-394 - ER: Related to the 506-byte Hero virus, but does not damage the files it infects. Awaiting analysis.

```
Hero-394       B98A 0133 C0BF 0002 0305 83C7 02E2 F929 069C 03B8 0042 33C9
```

Hungarian-482 - CR: This 482-byte virus from Hungary activates on November 7th. If an infected program is run on that date it will display the string 'Format ...' and proceed to format the hard disk.

```
Hungarian-482  5603 F7AC 0AC0 740A D0E8 B40E B307 CD10 EBF1 B901 00BA 8000
```

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**