April 1992 ISSN 0956-9979

VIRUS BULLETIN

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

CONTENTS

EDITORIAL

Michelangelo - A Post-Mortem

The Wogan Show, BBC1, 7.00 pm, Friday, March 6th 1992. Terry Wogan, the master of blarney, introduces his twice weekly chat-show by informing the studio audience that he has succumbed to the Michelangelo computer virus: 'I woke up this morning and it had painted my ceiling!' A feeble joke admittedly, but also the only Michelangelo virus story told that day which could definitely be discounted as nonsense.

The odd hermit or Trappist monk might have been unaware of the Michelangelo virus in the week running up to March 6th, but anyone else would be hard-pushed to plead total ignorance. Those unfortunate souls known to be involved in some way with computer viruses were bombarded with questions, not only from journalists, but from all quarters - a long-awaited pint in the pub turned into a thirty minute layman's guide to the PC bootstrap process for one unfortunate 'expert'. *Radio 1* ran regular news items, television bulletins showed the obligatory pictures of green caterpillars munching data and ASCII text avalanching down VDUs while a succession of 'experts' were wheeled out of semi-retirement to donate the necessary 'sound-bytes'.

Such a fever-pitch of media interest had been generated worldwide - early in February John McAfee of anti-virus software house *McAfee Associates* had been reported as saying that five million computers worldwide were infected. Whether McAfee actually said this or whether journalistic licence took its course is not known, but this single gross exaggeration is seen as the detonator which caused the media bomb to explode. Had five million computers genuinely been infected, the incidence of reported data loss would have been vastly greater than actually occurred. The important point is that data loss *did* occur, even after intensive media warnings. In other words, the threat was (and is) real but neither anti-virus software developers nor reporters should succumb to the urge to exaggerate it. In this instance, stating the simple facts would have been story enough. The British press, particularly those reports which appeared in *The Times*, *The Independent*, *The Guardian* and *The Observer* generally succeeded in telling the story accurately.

In the United Kingdom, *Total Control* was the first company to issue a warning; its press release in early February 1992 announced the availability of a free detection and recovery program. *Virus Bulletin* issued a press release on February 13th about Michelangelo. The release stated the following facts: the virus is destructive; it triggers on March 6th; it is relatively widespread; PC users are advised to detect the virus prior to the trigger date. Mercifully, the UK press, rather than assuming these releases to be yet another example of scaremongering or virus profiteering, decided to run the story; as events were to unfold these press releases and a subsequent press conference held by *New Scotland Yard's Computer Crime Unit* saved an untold volume of data from destruction.

The Michelangelo story was undeniably hyped. Exaggerated claims from the United States had fuelled the media frenzy and the admissions in February by US manufacturers *Leading Edge Products* and *DaVinci Systems* that both companies had shipped Michelangelo-infected disks (see *VB*, March 1992, p.3) served to heighten speculation about impending disaster. The virus had also been detected at university campuses throughout North America and Canada; the *New Jersey Institute of Technology* in Newark, for instance, detected the virus on 2,400 of its 3,000 PCs.

The fact that the virus was in circulation was undeniable; numerous organisations had reported Michelangelo infections. In the United States, *NASA* cleared 200 infected PCs prior to the trigger date, while State Secretary for Illinois George Ryan said officials had found and destroyed traces of the virus in the state's vehicle records office. Libertarians will be relieved to know that three of the four computers in use by the *New Jersey Commission to Study Sex Discrimination* were cleared of the virus before any damage could be done. Michelangelo was also isolated and cleared from offices in the United States *Senate*. In November 1991 the *Polytechnic of North London* announced that it had been hit (see *Case Study*, pp. 9). It is probable that a number of incidents were caused by infected Taiwanese software which had been imported into the UK in December 1991 (*VB*, February 1992, p. 2).

The Consequences

So what actually happened on March 6th and the days and weeks preceding it?

It appears that the anti-virus software developers had a field day. *Central Point Software* of Beaverton, Oregon, announced that sales of *Central Point Anti-Virus* had increased by 700% in the month preceding 'Michelangelo day'. On March 4th, giant US retailer *Egghead Software* announced that sales of anti-virus software were running 3,000% ahead of the previous week. A television report filmed at *S&S International's* Berkhamstead, UK, headquarters showed dozens of mailbags packed with *Dr. Solomon's Anti-Virus Toolkit* being loaded onto a mail van for despatch worldwide.

A number of companies (*Central Point*, *Symantec*, *Trend Micro*, *Total Control*) offered Michelangelo-specific detection and disinfection utilities. Ostensibly, these public domain utilities were offered as altruistic gestures but contained useful bait to prospective purchasers of the full-blooded commercial packages from which they originated. Three programs from *Central Point*, *Symantec* and *Trend Micro*, ranging in size from 90 to 121 Kilobytes, were made available on *Compuserve*. These unnecessarily bulky files were downloaded worldwide no less than 49,000 times.

A quick back-of-the-envelope calculation suggests that *Compuserve* stood to net at least $US90,000 from this exercise (assuming that all downloads were of the smaller program at 2400 baud and took place at the standard charge of 21 cents per minute).

The detection frenzy, stimulated by the media warnings, resulted in an increase in the number of virus infections reported to *VB* for the month of February 1992, a pattern which was presumably repeated across the anti-virus industry (see *Virus Prevalence Table*, page 6). In the desperate search for Michelangelo a diversity of viral flora and fauna was unearthed - February 1992 was the month in which PC Support worldwide conducted an early spring clean.

One ill-advised piece of advice was published in the 20th February edition of *Computing*. Mr. Michael Bacon, managing consultant at *Hoskyns*' IT security division was quoted as saying 'Obviously one way to check is to back up your system, move your computer clock to 6 March and see if you get this effect.' Three unfortunate people followed this detection methodology (needless to say, they ignored the reference to backups), and lost all their data.

United Kingdom

The first report which *VB* received on 'Michelangelo day' turned out to be the single worst incident of virus-inflicted data loss recorded so far in the UK. A non-disclosure clause prevents identification of the organisation concerned.

The incident had occurred at a site with approximately 2,000 PCs. Both IT management and PC Support personnel were fully aware of the Michelangelo trigger date due to the high profile media coverage in the weeks leading up to it. Moreover, the majority of machines had been checked using virus-specific scanning software and no Michelangelo infections had been detected. The detection software in use comprised obsolete versions of *Norton Anti-Virus* and *Dr. Solomon's Anti-Virus Toolkit* (the versions used were over 12 months old) and had been developed prior to the discovery of the Michelangelo virus in April 1991.

On the morning of March 6th, the virus triggered on more than 100 machines destroying an undisclosed volume of data. Updated detection software was couriered by despatch rider; the organisation faced the monumental task of detecting Michelangelo infection on the fixed disks of those machines that had not yet been powered up (see *'The Magic Object'*, *Technical Notes*, p.4). Moreover, tens of thousands of diskettes had to be checked to ensure that the virus would not re-enter the processing stream and cause similar chaos on March 6th 1993.

Two lessons can be learned from this incident:

- Virus-specific scanning software must be kept up to date. In this case a false sense of security was engendered by the use of hopelessly outdated software.
- In calculating the impact of this incident, data loss is but one factor in a subtle equation which includes the resources necessary to detect the virus on *all* magnetic media, the non-availability of systems while they are recovered, the man-hours involved in the recovery process and the commercial value of any data irretrievably lost.

There were other isolated incidents in the UK. *The Observer* newspaper (March 8th) interviewed Adrian Steel, the computer manager at a freight company in Tyne-and-Wear who had lost data on eight of the company's ten PCs. The machines contained company accounts and spreadsheets. Steel spent the weekend of March 7-8th attempting to salvage the records, most of which were irretrievable.

John Straker, a self-employed contract surveyor also decided to speak of his experience. He had all of his records, spreadsheets and correspondence destroyed by the virus. In this instance partial recovery proved possible (due to the availability of back-ups) but Straker still estimated the resulting financial loss at £3,000.

The *Computer Crime Unit* said that it had received reports of 117 personal computers being hit in dozens of companies across the United Kingdom. In a television interview shown on the evening of March 6th, Detective Inspector John Austen said that the impact had been more severe than expected but added that in the circumstances 'we have got off lightly'. *City University's* Andy Holt posted a note to the *CIX* bulletin board on 7th March to say that unprotected open-access machines on campus had been hit - in an admirable display of *sang-froid* Holt added: 'the lecturer responsible knew he was taking a risk and was philosophic about the result.'

Worldwide

Most reports of Michelangelo inflicted damage were relayed by the *Press Association*, *Reuters* and other professional news-gathering services. Paradoxically, the first report received was that the Uruguayan army had lost its counter-intelligence records. This story broke at approximately 8.30 a.m. GMT; considering that Uruguay is four hours behind GMT, this report appeared dubious. Interestingly, some machines in the United States, including those of the *Oakland Tribune*, were hit a whole day early due to the fact that 1992 is a leap year and this fact was not taken into account by some real-time system clocks.

Other confirmed casualties included an architectural firm in Japan which lost an estimated $29,000 of development work and a company in the Ruhr industrial belt which lost 75 machines. Reported incidents included some 48 Australian companies which were hit, while contaminated disks used to distribute specialised pharmaceutical software resulted in the virus triggering on approximately 1,000 computers at 450 firms across the Republic of South Africa. The United States was relatively unscathed - the incident which gained the most media coverage was that of a Southern Baptist church near

Atlanta, Georgia, which lost all of its data with no hope of recovery. In a rare corporate admission, financial trading house *Drexel Burnham Lambert* announced that two PCs had been hit at its offices in New York: hardly an earth-shattering revelation, but the company must be admired for its openness! *State Department* officials admitted on March 6th that the virus had struck IBM-compatible machines at three US missions: Toronto, Canada; Addis Ababa, Ethiopia; and La Paz, Bolivia.

John McAfee told *VB* that more than 1,000 companies had been hit in the United States and that the worst single incident involved twelve machines. McAfee added that the large corporate concerns had been the least severely afflicted and that it was the smaller businesses which reported incidents.

Steve White, Manager of IBM's *Thomas J. Watson Research Center* in New York painted a rather different picture - the *High Integrity Computing Laboratory* which White manages could verify only a single incident of the virus triggering within IBM's sample population which comprises several hundred thousand PC users chosen to reflect business computer use in the *Fortune 500*. White said that this finding did not necessarily conflict with McAfee's claims as the sample population was relatively sophisticated, being both aware of the virus threat and well protected from it. (Within IBM's sample population, virus incidents occur at a rate of 1 per 1000 PCs per quarter.) White said that the figure of a thousand disk drives failing on March 6th was perfectly reasonable but was this failure verifiably Michelangelo-inflicted? (The mean time between failures for hard disks varies between 10,000 and 50,000 hours.)

Aftermath

The projected figure of five million infected PCs worldwide which was widely reported by the press proved to have no statistical basis whatsoever. The extent of the cumulative damage caused by the virus on March 6th will never be fully known but appears to be relatively minor. However, as has come to be expected, certain organisations and individuals were hit with singular severity.

Much of the damage actually caused by the virus will be accounted for as hard disk failure or will simply go unreported. When a computer acts strangely or fails to work, the user is unlikely to contact a virus specialist immediately; he will turn instead to his PC dealer, the manufacturer of the computer, an engineer or others likely to overlook virus-inflicted damage.

In the light of the media warnings about the virus and its effects, it is amazing that so much damage *was* caused on March 6th. As a parting shot to the scaremongers - *there really was no need to hype this story*. Michelangelo remains a real threat and it caused severe damage on March 6th 1992, but only to a few unfortunate or negligent computer users. The overwhelming majority of PC users survived 'Michelangelo day' intact and they should be grateful to those responsible agencies which issued accurate warnings and to those journalists and editors who disseminated them.

Intel Tells All

In a supreme irony, the news broke on March 6th that *Intel*, a well-known semiconductor manufacturer which also markets software under its own name, had its own close encounter with the Michelangelo virus when the company shipped a consignment of infected diskettes from its warehouses.

The virus had contaminated some 839 5.25 inch diskettes shipped with version 3.01 of *LANSpool* 286 and 386 software. According to *Intel's* UK director of marketing, Sean Maloney, 180 infected diskettes were traced within Europe but some 650 diskettes had still to be recovered from North America. Any user who has received *LANSpool* 3.01 after 28th January 1992 is advised to contact *Intel UK Ltd* (Tel 0793 431144).

A toll-free hotline (800-228-4561) was set up in the United States to deal with enquiries and dedicated anti-virus software was provided free of charge. *Intel* also offered afflicted *LANSpool* customers a free copy of *LANProtect*, the company's server-based anti-virus system which retails for US$999!

Intel has not been able to ascertain how the virus infected the master diskette which was sent for duplication, but has not ruled out malicious tampering. An unspecified anti-virus package was in use but it failed to detect the infected master disk. In future, *Intel* plans to use the anti-virus software which it has reportedly licensed from *Trend Micro Devices* of Torrance, California.

TECHNICAL NOTES

The Magic Object

The Michelangelo virus yet again re-emphasises the vital importance of the **clean write-protected system disk** in combating virus infections.

If a PC boots from an infected disk on the trigger date of March 6th, the virus code executes the destructive trigger routine.

Organisations which lost a percentage of their machines on the morning of March 6th needed a guaranteed way of preventing the virus from triggering on suspect PCs which had *not* been switched on that morning.

The only way to prevent the virus code in the Master Boot Sector of the fixed disk from executing is to boot the suspect PC from the 'magic object' - the clean write-protected system diskette. Once the PCs were booted in this way, scanning proceeded and infections, where found, were cleared.

Date Tampering

A word of caution concerning the altering of system dates as a stop-gap measure to avoid damage by date-triggered viruses such as Michelangelo and Jerusalem. It is common practice for network file servers to set workstation time and date records when users log in. This can result in dates being reset without users being aware of it happening. Changing the file server date may get around this problem but may not be practical where networks are used for date-sensitive operations, such as accounting, payroll or invoicing.

Tampering with system dates is generally an ill-advised practice. Reliable detection and removal of any virus code is always the prescribed course of action. Infected hard disks have doubtless survived this year due to date tampering - however, the virus will trigger again next year and in the meantime these infected machines will continue to propagate the virus by infecting associated diskettes.

Double Trouble

A report in *The Times* (March 7th 1992) of PCs in the United States being hit early because they were infected by both the New Zealand II and Michelangelo virus is incorrect. The combination of these viruses does not change the trigger date.

The actual result of this combination is that the second virus to infect the PC superimposes the first virus over the only copy of the Master Boot Sector which will be stored in Track 0, Head 0, Sector 7. (Since both viruses relocate the code found in Track 0, Head 0, Sector 1 to Sector 7, the order of infection is irrelevant.) If trigger conditions are not met, the virus code in sector 7 will execute in a loop (it continually loads itself) and the machine will hang. However, on March 6th the destructive routine will activate regardless of whether Michelangelo is stored in sector 1 or 7.

Automatic disinfection routines do not usually account for cases of multiple infection. Simply copying sector 7 to sector 1 will **not** disinfect the machine - virus code will remain in both sectors. Disinfection can be achieved by restoring from a backup of the clean Master Boot Sector. Low-level formatting the hard disk and repartitioning is the only alternative.

Michelangelo: Further Details

1) The virus cannot infect 3.5 inch 720K disks as it assumes all disks other than 360K disks have at least 15 sectors per track. 720K disks have 9 sectors per track.

2) The destructive routine is triggered following a date check using INT 1AH function 4. This call was not serviced until the introduction of the IBM AT. Genuine IBM PCs and XTs do not support this call and the destructive routine cannot be triggered on them. Note that some PC/XT compatibles such as the Amstrad PC1640 do support this call and the Michelangelo trigger routine will function on them.

How Dangerous is 'Dangerous'?

It is common to consider 'disk trashing' viruses such as Michelangelo dangerous - but should this be the case? If backups exist, it is relatively easy to recover from an attack which formats or overwrites the hard disk. The real danger may lie elsewhere - those viruses which corrupt data in a subtle way, occasionally altering bytes or changing digits. Damage of this type may go unnoticed for a long time, the user being oblivious to the fact that spreadsheet data or other critical information is incorrect. When the virus is finally detected (possibly as the result of a disk-trashing routine) all existing backups may be corrupt. The dBASE virus was the first to demonstrate these insidious effects (*VB*, December 1989, pp. 9-10). Fortunately, it is not 'in the wild'.

Shirley Not!

David Chess of the IBM *T. J. Watson Research Center* has pointed out that the search pattern published for the Shirley virus in the February edition of *VB* produces a false positive in the German version of the *Norton Format Recover* program FR.EXE version 4.51. An amended pattern is published here:

```
Shirley  B887 4BCD 213D 6366 7566 2EA1 0E0E
         8CDB 01D8 0510 008E D02E
```

Hit-List

Several new viruses reported this month 'target' some specific anti-virus product. This is not a new development but one that is becoming more prevalent. Some viruses recognise the presence of a protection program and refuse to activate if it is found. In recent months the venerable *Flushot+* TSR monitor and *Central Point Anti-Virus* have been targeted in this way. Viruses may also tamper with the anti-virus program - possibly modifying the signature database it uses. There is no simple solution to this subversion, but one way to reduce the risk is to use scanners from several different manufacturers.

The Mutation Engine

The appearance of Dark Avenger's 'Mutation Engine' (MtE) is a significant development which will have a long-term impact on the development of virus scanners (see pp. 11-12).

Three viruses currently employ the Mutation Engine. Apart from their use of the engine these viruses are uninteresting - had it not been for the inclusion of the engine, few, if any, researchers would have expended serious work on analysing these viruses. However, many anti-virus companies have spent considerable effort in analysing the engine as it can be used to add complex polymorphic (variable encryption) ability to *any* virus. One MtE virus called Pogue is reported to be 'in the wild' in the United States.

A few scanners are now able to detect viruses which use the Mutation Engine and most scanners which are currently supported are expected to detect these MtE viruses soon.

Virus Prevalence Table - February 1992

Incidents reported to *VB* in the UK during February 1992.

Virus	Incidents	Total Reports
New Zealand II	11	20.3%
Form	11	20.3%
Tequila	7	12.9%
Michelangelo	4	7.4%
Spanish Telecom	3	5.5%
Cascade	2	3.7%
Vacsina	2	3.7%
Maltese Amoeba	2	3.7%
Flip	2	3.7%
Brain	2	3.7%
1575	1	1.8%
Jerusalem	1	1.8%
Nomenklatura	1	1.8%
DIR II	1	1.8%
Liberty	1	1.8%
Anticad 2576	1	1.8%
Joshi	1	1.8%
Total54	100%	

The reappearance of Brain in the above table, following a presumptious newspaper report that it was 'officially extinct', is reminiscent of Mark Twain's rejoinder: 'Reports of my death have been greatly exaggerated.'

DIRTY MACS

INIT 1984

A new Apple Macintosh virus designated INIT 1984 was discovered on Friday 13th March 1992. The virus triggers if an infected system is booted on any Friday 13th in 1991 or later years. Damage includes changing the names and attributes of folders and files to random strings and the deletion of a small percentage of files (less than 2%).

The virus only infects INIT files (or startup documents). It does not infect the system file, desktop files, control panel files, applications or document files. INIT files are shared less frequently than applications which will hinder its propagation.

Current versions of *Gatekeeper* and *SAM Intercept* (in both advanced and custom mode) are effective against this virus. Either program will issue an alert as the virus attempts to replicate. The virus infects all models of Macintosh. It spreads on *System 6* and *7* platforms. On older Macs, (those with 64K ROM), the virus will cause crashes at boot time.

Authors of all major Macintosh anti-virus tools are preparing updates to locate and eliminate INIT 1984. *Disinfectant* was upgraded to version 2.7 in late March 1992 and is available in the public domain courtesy of *Northwestern University* (ftp.acns.nwu.edu) and John Norstad. It is available via *Compuserve*, *Genie*, *Calvacom*, *MacNet*, *Delphi*, *AppleLink*, *American Online* and usual archive sites.

Version 1.2.5 of *Gatekeeper* (public domain courtesy of Chris Johnson) is also available via the standard archive sites including microlib.cc.utexas.edu, sumex-aim.stanford.edu, rascal.ics.utexas.edu and comp.binaries.mac.

Symantec's SAM (*Virus Clinic* and *Intercept*) has been upgraded to version 3.0.7 which is available immediately from *Compuserve*, *American Online*, *Applelink* or from the *Symantec* BBS 408 973 9598. *Virex* from *Microcom* (919 490 1277) has released version 3.7 of *Virex INIT*. All *Virex* subscribers will be sent an update on diskette. Other registered users will be sent updated scan data which can also be viewed on *Microcom's* BBS (919 419 1602).

Virus Detective (shareware supported by Jeff Schulman) has been upgraded to version 5.0.3. The search string is:

```
Resource INIT & Size<4500 & WData 494E EA994*4954
8A9AB ; for finding INIT 1984
```

Acknowledgements to David Ferbrache and Professor Gene Spafford.

Microsoft Word Sets A Bad Precedent

Bob Jones of *Queen Mary's University*, London, raised an interesting 'attitude' alert in a recent posting on *JANET*. His concerns surrounded the documentation released with *Microsoft's Word* version 5.0 for the Macintosh. Page 12 of the 'Getting Started' manual states that prior to installation the user should 'disable any virus protection programs. For example, if you are running *Gatekeeper*, you must remove it from the System folder and restart your computer.'

Combined with *Microsoft's* usual disclaimer 'MICROSOFT AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY OTHER DAMAGES WHATSOEVER...ARISING OUT OF THE USE OF OR INABILITY TO USE THIS MICROSOFT PRODUCT...', this requirement leaves the user absolutely defenceless against virus or Trojan activity - such programs may only activate when protection software is not running!

Microsoft is a reputable company which takes enormous care to ensure that its products are virus-free. Automated installation processes are a desirable feature but the insistence that protection software be disabled in order to facilitate installation is setting a very bad precedent indeed. It will inculcate the erroneous belief that it is safe to install shrink-wrapped software without anti-virus protection. Considering the recent litany of shrink-wrapped virus accidents this disturbing development is to be resisted.

IBM PC VIRUSES (UPDATE)

Updates and amendments to the *Virus Bulletin Table of Known PC Viruses* as of 23rd March 1992. Hexadecimal patterns may be used to detect the presence of the virus with a disk utility or preferably a dedicated scanner.

Type Codes

C = Infects COM files **E** = Infects 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

R = Memory-resident after infection **P** = Companion virus **L** = Link virus

Seen Viruses

AntiCAD 3088 - CER: The latest member of the AntiCAD/Plastique family. It is 3088 bytes long and is detected by the same pattern as the 2576 byte variant.

Antimon - CN: This 1450 byte virus has also been named Pandaflu, because it is targeted against *Flushot+* and some programs from *Dr. Panda Software*.

```
Antimon         83C2 102B D033 C9B8 0042 CD21 BA00 01B9 AA05 B440 CD21 5A59
```

AT - CR: This is an old group of viruses which are rather inefficient infectors as they only work on the 80286 processor and above.

```
AT-144          0042 33C9 CDB4 B440 8D54 FFB1 0389 2CCD B4B4 3ECD B41F 61EA
AT-149          33C9 33D2 CD21 B440 8D54 FFB1 0389 2CCD 21B4 3ECD 211F 61EA
AT-132          B800 428B CACD E5B4 40B2 2DB1 0389 2CCD E5B4 3ECD E51F 61EA
```

CAZ-1159 - CER: Similar to the 1204 byte variant and detected with the same pattern.

Dedicated - CN: This virus employs 'The Mutation Engine' as a means to variable encryption (see *Technical Briefing*, pp. 11-12). No search pattern is possible.

Demolition - CR: A 1585 byte encrypted virus which contains destructive code, as well as various text messages.

Fear - CN: This virus employs 'The Mutation Engine' as a means to variable encryption (see *Technical Briefing*, pp. 11-12).

FGT - CN: 651 bytes. Awaiting analysis.

Forger - EN: A 1000 byte virus which causes subtle corruption - occasionally modifying a byte on the disk.

```
Forger          215A 520E 1F5F 0706 57B8 0000 B980 00F2 AE47 83F9 0075 03E9
```

Gliss - CN: A German 'demonstration' virus which does nothing but replicate.

```
Gliss           218B D85F 578B 45FC 0527 00BF 0401 8905 B906 00BA 0001 B440
```

Got You - EN: A 3052 which contains code to overwrite critical portions of the hard disk. Awaiting full analysis.

```
Got You         6C00 4000 C5AA FFF0 413A 0034 122A 2E2A 0047 204F 5420 594F
```

Hafenstrasse-791 - EN: Very similar to the original variant and detected with the same pattern.

Japanese Christmas-Cookie - CN: This 653 byte variant of the Japanese Christmas virus has been modified to display the messages 'Give me a Cookie' and 'Cookie'.

```
Jap-Cookie      1B90 32E4 CF50 528A 1446 80F2 FE74 06B4 06CD 21EB F25A 58C3
```

Jerusalem-2187 - CER: Yet another Jerusalem variant 2187/2189 bytes long.

```
Jerusalem-2187  2638 05E0 F98B D783 C203 B800 4B06 1F0E 07BB 4600 1E06 5053
```

Jerusalem-Mummy - ER?: This 1489 byte variant seems only able to infect EXE files. It contains an encrypted text string which claims it is written in the *Kaohsiung Senior School*. Awaiting full analysis.

```
Jer-Mummy       2638 05E0 F98B D783 C203 B800 4B06 1F0E 07BB 9A04 9C2E FF1E
```

Kalah - CR: This 390 byte virus is quite harmless - it does not have any effects other than displaying 'VDV 91'.

```
Kalah  B43F     CD21 8B0E 0000 2E3B 0E00 0175 0B8B 0E02 002E 3B0E 0201
```

Macedonia - CR: One of the few viruses which carry a political message - 'MacedoniaToTheMacedonians'. This 400 byte virus has no effects other than displaying this message.

```
Macedonia       7527 E871 002E 8B04 2EA3 0001 2E8B 4402 2EA3 0201 0E0E 1F07
```

Mannequin - CER: A 778 byte virus which has only one unusual effect. It intercepts INT 17H (the printer interrupt) and strips the top bit of any character sent to the printer.

```
Mannequin       5251 5350 32C0 1E07 8BFA B941 00FC F2AE 83EF 0C8B F70E 07BF
```

Mosquito-Pisello - ER: 1024 bytes long, similar to the original variant but awaiting full analysis.

```
Pisello         5650 BE51 032E 8A24 2E32 265D 012E 8824 4681 FE7A 0375 EE58
```

Mshark - CN: The name of this 373 byte virus is derived from the text string '(C) Mshark-S v.1.0'. This is a simple virus, with no side-effects.

```
Mshark          0103 D6CD 2132 DB56 81C6 5601 B914 00AC 3413 02D8 E2F9 5E38
```

Nines Complement - CR: This 705 byte virus interferes with printer operations, changing numbers so that 0 becomes 9, 1 becomes 8, 2 becomes 7 and so on.

```
Ninecomp        E800 005B BE11 0003 F3B9 AA02 89F7 AC30 D8AA E2FA
```

Nov 17. - CER: As the name indicates, this virus activates on 17th November, trashing the beginning of the current drive.

```
Nov 17.         B42A CD21 80FE 0B75 1280 FA11 720D B419 CD21 B908 00BA 0100
```

Pc-Flu 2 - CER: This virus was described in *VB* last November, but several new versions have now appeared. Just like the original virus they require an algorithmic detection method.

Peach - CER: This 887 byte virus is targeted against *Central Point Anti-Virus*. Its name is derived from a text string found inside it - 'No 2 Peach Garden'.

```
Peach           33C9 33D2 E851 FFB4 40B9 1800 8BD7 807D 015A 7406 B913 00BA
```

Phoenix-2000 - CR: This is a polymorphic virus which cannot be detected with a simple search pattern. In addition to infecting COM files, it Trojanises EXE files - overwriting them with code to trash a part of the hard disk. This Trojan can be detected with the following pattern:

```
Phoenix-Trojan  B413 CD2F 06B0 F5E6 6033 C0E6 618E C093 AB58 ABBA 8000 B901
```

Pixel-Pixie 1.0 - CN: This virus is closely related to the Pixel-936 virus, and detected with the same pattern.

Pogue - CR: A variant of the Gotcha! virus which employs 'The Mutation Engine' (see *Technical Briefing*, pp. 11-12).

Sadist - EN: This 1434 byte virus does not seem to do anything but replicate.

```
Sadist          2EC6 045C B908 0046 4526 8A46 002E 8804 E2F5 2EC6 4401 008D
```

Smiley - CN: A 1983 byte virus which contains code to trash the hard disk. Awaiting full analysis.

```
Smiley          BB05 018B C881 E10F 00D1 E8D1 E8D1 E8D1 E883 F900 7401 4089
```

Squawk - CER: A 852 byte virus from Asia, which is easy to detect, as an infected machine will emit a high-pitch sound.

```
Squawk          4B8E DBA1 0100 0306 0300 3B06 1200 722F 812E 0300 0001 812E
```

Tabulero - ER: A 2048 byte virus which bears some resemblance to the Jerusalem virus but which is not directly derived from it. Awaiting full analysis.

```
Tabulero        2E8B 4702 2E89 052E 8B47 042E 8945 022E 8B47 062E 8945 0433
```

Timid - CN: Two variants of the *Little Black Book* viruses are now known - 305 and 306 bytes long. Both are very obvious but as the source code is available from *American Eagle Publications Inc*. (*VB*, March 1992, pp. 17-18) they can be modified easily.

```
Timid-306       8B16 FCFF 83C2 00B9 3F00 B44E CD21 0AC0 750B E809 0074 06B4
Timid-305       8B16 FCFF B93F 00B4 4ECD 210A C075 0BE8 0900 7406 B44F CD21
```

TV - ER: A 730 byte virus, which has also been named Ontario-730, but this name was rejected because the virus is not related to another virus named 'Ontario'. Awaiting full analysis; it contains code to trash the hard disk.

```
TV-730          BF00 01B8 6E4B CD21 3D54 5675 0AC7 05EB 59C6 4502 90FF E78C
```

Vienna-712 - CN: Another Vienna variant, 712 bytes long and detected with the previously published Vienna-4 and Dr. Q. patterns.

Vienna-534B - CN: A member of the W-13 group in the Vienna family closely related to 534A and detected with the previously published W-13 pattern.

Vienna-644B - CN: Related to the original 648 byte variant, but shorter. Detected with the previously published Vienna-1 pattern.

Vienna-645B - CN: Closely related to the Vienna-645 virus. Detected with the Ghostballs pattern.

CASE STUDY

David Bell
Network Manager
Polytechnic of North London

Combating Viruses in the Polytechnic of North London

The UK's universities, polytechnics and institutes of higher education are engaged in what can only be described as a relentless war against virus contamination and damage. In the autumn of last year the Polytechnic of North London was one of the first sites in the United Kingdom to encounter the notorious Michelangelo virus when a large number of machines became infected. In this case study, David Bell, the Polytechnic's Network Manager discusses this outbreak, the hazards of academic computing generally and the tools, tactics and techniques he uses to wage anti-virus warfare.

Irritating Diversions

Viruses are a pain. I would much rather be testing *Windows 3.1* or setting up a multi-media system than spend valuable time fighting viruses, but needs must.

I have been responsible for protecting the machines within the Polytechnic since 1990. In March of that year we encountered the Jerusalem and Stoned viruses. The tools for protecting our machines were very limited; we used *SCAN* to detect the infections and *UNVIRUS* and *HCRACK* to remove them. It was a very time-consuming and laborious task. Every machine had to be checked by a member of the systems team. Then there was the problem of how to clean all the infected floppies!

Viruses weren't our only problem. Students love to experiment (I just wish they only did it in their own rooms). They want to find out what happens if you delete COMMAND.COM! They want to load their own games and so will delete the application needed by the class taking an exam the next morning. I had to find a way to prevent files from being deleted.

We also have many students new to computers and they need a simple-to-use menu system rather than the DOS interface which could hardly be described as user-friendly.

For us the answer to these problems was *PCGUARD* (now called *Flexiguard*) from *PC Enhancements Ltd.* This product initially just addressed our file protection and menu needs. It was later developed to protect against viruses as well.

We installed *PCGUARD* on all of our student access machines and used the McAfee *SCAN* program to check the hard disk on each reboot of the computer. This took between one and two minutes depending on the number of applications loaded. I was expecting howls of protest from both students and staff; but they all accepted the overhead as a necessary fact of life in this virus-ridden age.

So far so good. *PCGUARD* did a reasonable job of protecting the application directories and the menu system worked well. The level of support call-out dropped dramatically. Everything seemed under control.

Learning the Hard Way

Let what happened next be a lesson to us all. The systems had been so secure and we had so much other work to do during the summer of 1991 that we did not update the scanning software on any of our open access computers before the students returned for the new academic year.

The term started quietly. Then reports of a new, unspecified virus started to filter through to us. This virus spread very rapidly and when I inspected the afflicted building all the machines in two rooms had been infected and a third room was being attacked. This third room had the new *Flexiguard* program installed on machines just commissioned that summer, but the other two rooms contained older machines dependent on the now out-of-date scanning software.

Using an updated scanner the new virus was identified as Michelangelo and it had infected all 46 machines 'protected' by the obsolete software. It also infected the machines protected by *Flexiguard*. These machines reported the infection on the next reboot and locked, preventing the further spread of the virus.

"This virus spread very rapidly and when I inspected the afflicted building all the machines in two rooms had been infected and a third room was being attacked."

The students were concerned by this Michelangelo infestation. They were desperate for information on how to protect their data. A few bought commercial detection software out of their grants. Some students even destroyed infected floppies.

At this point I managed to persuade senior management to allocate the funds necessary to install virus protection on all 250 student access machines and the 550 staff machines. [According to the March 12th edition of *Computer Weekly*, the *Polytechnic of North London* has spent £22,000 on anti-virus software. Ed.]

We instigated an immediate project to clean all the machines and install software which enabled students to remove Michelangelo infections from diskettes. We also configured the menu system so that before an application could be run the students had to load the floppy disk (containing their data) and have it scanned.

The main software used in this process was McAfee's *SCAN* and *CLEAN*. Whenever an infected disk was discovered, *CLEAN* was used to remove the virus. This was almost 100% effective - the occasions when it failed were when a floppy was infected by both Michelangelo and Tequila (see '*Double Trouble*' *Technical Notes*, p.5). In these cases we copied the files to another diskette and reformatted the original.

Once all student machines were protected, the number of infected floppies gradually decreased. The workload on ourselves was also reduced as the students themselves became proficient at cleaning their diskettes.

The Virus Protection System

My next problem was protecting the staff machines. Our staff users are not computer experts. They know enough to operate their word-processor or terminal emulation package but little more. How was I going to get them to protect their computers against the virus threat?

I decided to generate a system that would be easy to install. The *Virus Protection System* (*VPS*), as I called it, was based on the *VIS* set of programs. Use of these programs is free in the academic community. However, I also used one program from the *Flexiguard* suite.

We generated *VPS* disks pre-installed with DOS (we had to have disks with all versions from 3.21 through 5.00) and the anti-virus programs. The users were told to put the disk in the A: drive, power-cycle their computer and then type 'install'.

The install program scanned the hard disk (I used *VISCAN* for this) and if all was clean, it copied itself to a new directory on the C: drive. The system then modified CONFIG.SYS to start up *VISMON* (a memory-resident virus-specific monitor) as a device driver. It also modified AUTOEXEC.BAT to run *MCLEAR* and *VISCHECK*.

MCLEAR is a program which generates a checksum of the memory in the computer after DOS has been loaded. The checks are more complex than a simple sum of the memory locations. The first time *MCLEAR* runs it writes the calculated values to a file. Upon every subsequent restart it checks memory for any changes by comparing with original checksum values in this file. This program is essential to ensure that a virus has not been loaded with DOS. With *MCLEAR* I am able to run scans, having booted from the hard disk, reasonably confident that a virus is not already in memory.

The install process uses *VISCHECK* to generate files with checksum information about all EXE and COM files. The modifications to AUTOEXEC.BAT cause *VISCHECK* to be run once a day to ensure that executable files have not been modified by a virus missed by *VISMON*.

This system when properly installed is a good protection against viruses. But how do you get it installed on 550 PCs?

I made the system available in all buildings from the Computer Services Representative and put up notices in all areas. Very few people came forward to get a copy.

Of those that did install the system there have been a few complaints about the error messages reporting when files have been deliberately added or deleted from the hard disk. I provided a system to recalculate the *VISCHECK* files after scanning the entire hard disk for known viruses. This takes a long time. I will bring out a new version of *VPS* which will reduce the frequency with which COM and EXE files are checked. It should also make it easier to generate new checksum files when programs are added or deleted.

I recruited a student to send out copies of the system to key managers and to offer help with the installation. She had a very hard time, people were suspicious and unhelpful. They could not see why it was necessary or claimed that their computers were never used by other people, so how, they argued, could the machine become infected?

Judgement Day

What finally convinced nearly everyone about the threat was the publicity over the Michelangelo virus. The reports in the papers and the national television and radio news alerted everyone to the imminent trigger date of March 6th. In the two days preceding 'Michelangelo day', I telephoned every number in the Polytechnic's internal telephone book. I told everyone that they might lose their hard disks unless they installed the *Virus Protection System*. We were very busy. Eight systems were found to be infected by Stoned and there were a few PCs infected with Jerusalem. Miraculously, there were no Michelangelo infections.

On the morning of March 6th I was worried, I answered every phone call with trepidation; would someone lose their research data? We had done all that we could but there might still be a machine somewhere... In the event we were extremely lucky and not a single machine was hit.

Software and Suppliers

Flexiguard	*PC Enhancements Ltd.* Telephone 0707 59016
VIS Utilities	*Total Control Ltd.* Telephone 0488 685299
SCAN	*International Data Security Ltd.* Telephone 071 631 0548

TECHNICAL BRIEFING

Fridrik Skulason

The Mutation Engine - The Final Nail?

Last year a note was posted on *FidoNet's* virus conference, where 'Dark Avenger' announced his soon-to-be-released Mutation Engine (see *VB*, April 1991, p.19). He has now done so - releasing the engine with documentation, sample code and he even offers technical support via a virus exchange BBS in Bulgaria. [*Dark Avenger's tech support is presumably better than that offered by certain anti-virus vendors - see this month's survey, pp. 17-24. Ed.*]

The Mutation Engine is a logical extension of the process which began with the 1260 virus (*VB*, March 1990, p. 12, April 1990, p. 10). In that exercise the author (Mark Washburn) proved the possibility of variable decryption whereby no code remained static as the virus 'copied' from file to file. At the time 1260 was cited as the 'first nail in the coffin of virus-specific detection'. For certain simple scanning products, the Mutation Engine may well prove to be the final nail.

The current version of the engine (MtE 0.91) contains the following files:

MTE.OBJ	The main engine
MTE.DOC	Documentation
DEMOVIR.ASM	The source to the 'Dedicated' virus
DEMOVIR.OBJ	Same, in object form
RND.ASM	Source code to the random number generator
RND.OBJ	Same, in object form
MAKE.BAT	Used to create an executable virus
NOPS.BIN	Data file
READ.ME	Some comments from the author

The whole package might best be described as a virus writers' 'Toolkit', the intention being that a virus writer can utilise the Mutation Engine via a single subroutine call thus rendering his code extremely difficult to analyse and detect. The generic term for viruses which demonstrate the encryption processes used in the Mutation Engine is 'polymorphic'.

The documentation is quite interesting to read. The following excerpts are reproduced exactly from file MTE.DOC:

```
1. Licence
You are free to include this Engine in viruses.
Using it in another ways is prohibited. You are
free to give it to people that will only use it in
this way. MuTaion engine is free.

2. How it works
Please read the whole document before trying to do
something with the Engine. If you have never
written a virus in Assembler, DON'T start with the
Engine. First do this, then return back to the
Engine.

MuTation Engine is an object module that could be
linked to any virus. It has been written in
Assembler and assembled under Turbo Assembler 2.5.
We recommend that you use this assembler to compile
the viruses that will carry the Engine. Linking it
to an object file produced by other assemblers, or
high-level languages compilers is theoretically
possible, but we never tried and do not recommend
it. We decided NOT to give up the Engine's source
code at this time.

The Engine will encrypt your code each time with a
different encryption key. It will also generate a
routine to decrypt it, which will also differ each
time. Both the decryption routine and the encrypted
code will have variable lengths. Thus your virus
will be hardly detectable. The Engine's code is
about 2KB; we believe this is not too big.
```

To say the decryption routine 'differs each time' is an understatement - the code produced by the engine is far more complex than the code which Whale (*VB*, November 1990, pp. 17-20) and V2P2 (*VB*, pp. 18-20) generate. It is totally impractical to attempt detection with a set of signature strings (i.e straightforward hexadecimal patterns) - the code is simply far too variable.

Structurally the decryption routine can be divided into the following five steps:

Step 1: Generate a pointer to the start of the encrypted code. This may be done with a simple instruction such as 'MOV BP,1F4B', but probably a more complex method will be used, such as:

```
MOV AX,8DEE
MOV DX,184B
MUL DX
MOV DI,AX
```

Step 2: Generate a decryption key. Again, this may be done with a single instruction, but also with a long, complicated sequence.

Step 3: Decrypt a word. This is only rarely done with a single instruction such as XOR [DI+0CEA],BX, but usually in a convoluted way, such as:

```
MOV AX,[BP+0D22B]
SUB AX,SI
MOV DX,7D67
MUL DX
MOV DX,7E3B
MOV CX,AX
MOV AX,2386
SUB AX,CX
XCHG AX,CX
XCHG AX,[BP+0D22B]
```

Step 4: Increment the pointer register. This is quite often done with just two INC instructions, but as one would expect, much more complicated ways may be used as well.

Step 5: Branch back to step 2

Significance and Implications

At the moment three viruses are known which use Dark Avenger's Mutation Engine. They are Dedicated, Fear (a variant of Dedicated) and Pogue (which belongs to the Gotcha! family). The latter virus contains a text string 'TNX2DAV' - Thanks to Dark Avenger.

The appearance of these viruses is not particularly significant. What *is* significant is the availability of the engine *itself* and the fact that virus writers are *already* using it in order to conceal their code. It is inevitable that a series of MtE-encrypted viruses will appear in the near future.

As long as Dark Avenger does not release the actual source code, any anti-virus program which detects the current MtE viruses should also be able to detect any new ones. However - the current version is only 0.91 - which indicates that version 1.00 is under development. There are numerous ways in which the engine could be 'improved' - for obvious reasons they are not listed here.

As would be expected, anti-virus products written before the release of the Mutation Engine were generally ineffective in detecting it. Integrity-checking programs such as those which use cryptographic checksumming were of course able to catch it, *after* it had infected files, but all existing scanners will have to be updated. A handful of static analysis tools were able to determine the presence of highly suspicious self-modifying code in files containing the engine.

Detecting the current version of MtE is not easy - at least not without running the risk of causing regular false positives which will prove unacceptable to the end-user.

A Torture Test

Perhaps the appearance of the Mutation Engine should be considered a torture test for the *R&D* departments of all the anti-virus companies - if they are not able to detect it in a couple of months they would be well advised to redirect their efforts to other pursuits.

Anti-virus programmers (and teams) are already stretched - the Mutation Engine may well be the straw that breaks quite a few camels' backs. This is the technical editor's personal opinion, but those who disagree are reminded that, even now, some 18 months since its development, only about half of the virus scanners on the market detect V2P6 with 100% consistency and the encryption used in Mr. Washburn's V2Pn series is orders of magnitude simpler than that used in Dark Avenger's Mutation Engine.

VIRUS ANALYSIS

Jim Bates

Plastique 5.21 virus (aka Invader, Mozart)

This virus has been reported at large in the UK and at several locations across Europe. It is thought to have originated in Taiwan or China and appears to be the latest in the series of AntiCAD/Plastique viruses.

The major point of this series of viruses is that they are targeted to cause trouble only to users of the *AutoCAD* Computer Aided Design program. Earlier versions of this virus simply deleted the ACAD.EXE file but this one is more subtle (see below). Other added features include a 'musical' routine and an added boot sector infection capability. The first part of the virus code is encrypted, but once decrypted, various text strings can be seen. These include the file names ACAD.EXE and COMMAND.COM and the message:

```
by Invader, Feng Chia U., Warning: Don't run
ACAD.EXE!
```

During disassembly, I was interested to find a familiar old routine for sending frequency and duration information to the sound channel. This routine has obviously been lifted from an early IBM demonstration file but for some strange reason the virus writer had decided to encrypt the musical data which is processed by the routine.

Musical Appreciation

Once decrypted and processed, the tune is revealed as an appalling approximation of the introductory theme to the first movement of *Mozart's Symphony No. 40* (K.550) in G Minor. This is a symphony which was originally scored for a flute, two oboes, two clarinets, two bassoons, two horns and strings. It is therefore perhaps expecting rather a lot that a retarded virus writer could hope to achieve much through the 2.5 inch speaker of a PC's sound channel. Nevertheless, the essential spirit of one of Mozart's most original thoughts could have been captured a little more closely if the author had paid sufficient attention to the plain mechanics of this most precise of opening themes. To paraphrase a famous Stan Freberg comment - 'You can bugger up programs 'n you can bugger up files buddy, but don't you bugger up Mozart!'. (There is a report from the United States that a version of this same virus exists with the music changed to the theme from the television series 'Sledgehammer'.)

Structure

This is a multi-partite virus, infecting both COM and EXE files as well as disk boot sectors. The infective length of the virus on files is 4096 bytes, while the boot infection incorpo-

rates the whole virus which resides in the DOS Boot Sector rather than the more usual Master Boot Sector. The virus code becomes memory-resident when an infected file is executed or when the PC is booted from an infected disk. The virus hooks interrupts 08H, 09H, 13H and 21H.

Installation From a File

At the virus entry point, a routine is called which checks to see whether the virus is currently resident and active. The virus places a value of 4243H into the AX register and issues an INT 21H function request. If the virus is active, a value of 5678H is returned in AX. If the virus is detected in this way, a special function call of 4244H is issued. This is handled by the virus and control passes to the current program.

If the system is not infected, a virus stack is set up and 424 bytes are decrypted from the 80th byte of the virus code onwards. This area contains the text and the musical data.

After the decryption, a routine is executed which determines the speed of the processor and this value is used to compensate the speed of the music routine later. Then various calculations are made to make space available in low memory for the 4096 bytes of virus code. The move to low memory is achieved by poking three bytes into address 0000:03F0H and jumping to it. The three bytes comprise a repeat move instruction and then a far return. After execution this memory area is restored to its original values. Once processing enters the low memory code, the interrupt handling routines for INT 21H (DOS Service), INT 08H (Timer Tick), INT 09H (Keyboard BIOS) and INT 13H (Disk BIOS service) are hooked into the system using the standard DOS GETVECTOR and SETVECTOR function calls. Finally, a LOAD and EXECUTE request is issued via the original INT 21H vector and the host program is executed as a child process. Once the host exits, the virus regains control and returns to DOS via a legal TSR function call 31H.

Installation From a Boot Infection

When the PC is booted from an infected disk, the virus installs itself in high memory by the more usual expedient of decrementing the Top of Memory pointer (in this case it subtracts 5k from memory) and then loads its code from the disk into this space. The boot code contains an additional INT 08H handling routine which is simply a monitor to ensure that the virus only attempts to hook the INT 21H vector after the system has loaded. Once this installation is complete, it requires the execution of an infected file to reset the original INT 08H handling routine which controls the music.

Infection of Files

This occurs during the interception of a LOAD AND EXECUTE request (4B00H) or an OPEN for ReadOnly request (3D00H). Thus any executable program, even within a *Windows* environment, may be a target for infection.

The virus ensures that COMMAND.COM is not infected and neither is ACAD.EXE although an execution request for the ACAD file is not completed. If an EXE extension is found, a flag is set but no check is made for the MZ header. Infected files are recognised by the presence of the value 1990H at offset 12H into the file (this is the checksum field in EXE files). Infected COM files grow by 4096 bytes and EXE files by between 4096 and 4110 bytes. Since this virus has no stealth capability this change in size is easily detected.

Infection of Disks

This is handled by the virus INT 13H routine which intercepts only read requests and checks for hard disk access. The routine itself maintains a counter which is checked whenever a request to read the DOS Boot Sector (on fixed or floppy disk) is received. If this counter does not have a value of 2, it is incremented before the request is allowed to continue. Thus every second access of any DOS Boot Sector will result in the execution of the infected boot code. This works differently on floppy and fixed disks. On floppy disks, an extra track is formatted beyond the normal end of the disk (track 41 or 81 depending upon the media). The newly formatted track has 9 sectors and will contain the whole of the virus code in addition to its code already stored in logical sector 0.

On fixed disks, the virus is written to the DOS Boot Sector. This is usually (but not always) found on Track 0, Head 1, Sector 1. This should be noted by anti-virus researchers since it is unusual for a virus to infect the DOS Boot Sector without touching the Master Boot Sector (Track 0, Head 0, Sector 1). The original DOS Boot Sector is relocated to Track 0, Head 0, Sector 15. The remainder of the virus code is written to Track 0, Head 0, Sectors 7 through 16 (sector 15 excluded).

Trigger Routine

The trigger routine is particularly vicious.

When the Ctrl-Alt-Del key combination is pressed to force a warm reboot, the INT 09H keyboard intercept routine recognises this and invokes a selection routine depending upon several factors - how many files have been infected, whether the music is playing and how long before the play cycle is resumed. This means that the trigger routine will not occur at every Ctrl-Alt-Del and the odds are difficult to calculate with any accuracy. However, when it does activate, the trigger routine will attempt to overwrite every sector of every head of every track of the first two floppy drives and the first two fixed drives with the 'Invader' message noted above, together with the virus code and associated garbage beyond the code ending in memory. Once this trigger executes, recovery is not possible!

Disinfection

Once installed, the virus will play the famous Mozart theme at half-hourly intervals - i**f you hear it, do not attempt a warm reboot i.e. Ctrl-Alt-Del**!!!

Switch your machine off and then reboot with a clean system disk before you begin investigations.

A reliable hexadecimal detection pattern for this virus was published in *VB*, July 1991 and is repeated here:

```
Plastique  5.21  0681  002E  8C06  8500  2E8C  0689
                 008C  C005
```

Infected files should simply be deleted and replaced from clean write-protected master software or clean write-protected software backups. Note: All infected files must be deleted. For maximum security, infected files should be positively erased by multiple overwriting prior to their deletion. This will prevent undesirable 'resuscitation' by the inquisitive!

Disk editing tools such as *The Norton Utilities* can be used to disinfect hard disk boot sector infections. An infected DOS Boot Sector (usually, but not always, located at Track 0, Head 1, Sector 1) may be cleaned up by replacing it with the original DOS Boot Sector which is stored at Track 0, Head 0, Sector 15. Note that this assumes a sector size of 512 bytes; differing sector sizes should be calculated accordingly.

An alternative and easier method is to use the DOS *SYS* command (boot from a clean system disk containing the *SYS* program and type SYS C:). This replaces the operating system on disk and disinfects the boot sector by overwriting the virus with a clean DOS Boot Sector.

Diskettes should be disinfected only after the machine has been booted from a clean DOS disk. Data should be transferred from the diskette using the DOS *COPY* command. The diskette should then be formatted. Note: do not use *DISKCOPY* to transfer disk contents as this is an image copier which will transfer the virus code in logical sector 0.

Plastique 5.21

Virus Name - Plastique 5.21 (aka Invader, Mozart)

Infects - COM files (except COMMAND.COM), EXE files and DOS Boot Sectors on fixed disks and hard disks

Infective length - 4096 bytes (COM)
4096-4110 (EXE)

Avoids - COMMAND.COM and ACAD.EXE

Self check - put 423H into AX and call INT 21H - 5678H is returned in AX if virus is resident

Trigger - Ctrl-Alt-Del (warm reboot) causes the virus to trash drives A, B and C, overwriting all tracks, heads and sectors

✉ LETTERS

From Dr. Frederick B. Cohen

I was surprised to see someone who wants to maintain a reputation for accuracy and integrity as Jim Bates attempt to rewrite history in his letter to the editor in the last *VB*.

Jim's characterization of my contributions regarding computer viruses is not only inaccurate, but it verges on slander. It is negligent as well, since Jim Bates should know full well that his characterization of my research was false and misleading. I notice also that Jim Bates is on the editorial board of your ever more rag-like magazine, and as such, his opinions appear to reflect the official position of *VB*.

Jim seems to leave the implication in his letter that I have published the source code of computer viruses and that this makes me somehow responsible for them. In fact, it is just the opposite. I am one of the authors of books on computer viruses that uses only pseudo-code. The purpose is to teach you what you have to know without providing an easy method of attack. Jim probably read about another author's book and assumed that I did the same thing. I am not responsible for attacks, but I am responsible for most of the defenses on the market today.

Let me summarize a few of the contributions left out by Jim. I defined the term, and proved that modern protection systems were inadequate. In the process, I provided the first examples of virus defenses, described how they worked, and demonstrated their limitations. Every virus scanner on the market today is based, at least to some degree, on the virus detection example in my first paper on the subject.

I was the first to propose using cryptographic checksums for virus detection, and invented and then subsequently proved the utility and cost-effectiveness of integrity shells, which formed the basis for all of the resident virus monitors, resident checksum systems and similar protection techniques now in widespread use. My *Integrity Toolkit* product (which *VB* has refused to review for no specific reason) and which won the 1989 *Information Technology Award* as the best anti-virus initiative had these capabilities fully some three years before any competitor introduced them.

In response to the idea of a stealth virus (which I also introduced in theory several years before they appeared in the wild), I introduced a very strong defense (called the *SnapShot*) which is now increasingly used in commercial products.

I have published nearly 80% of the refereed technical papers on computer viruses and so cannot even start to describe the many contributions I have made in the virus protection arena. I am not some crackpot (as Jim Bates would have you believe) who made a reputation by attacking systems! All of my experiments were authorized and well controlled. If Mr. Bates, who seems to claim expertise in this area, would bother

to read the research results I produce, and assuming he took the time and effort to understand them, he would probably not make such ridiculous assessments and proclamations.

As to the history of benevolent viruses, the first ones were introduced by John Von Neumann over 60 years ago in his initial papers on computing, and have been the subject of many research papers on computing. There are about 100 research projects ongoing all around the world in this area, and the results have been published over a substantial period of time. The first widely available commercial product based on benevolent viruses was introduced this month. It automates many aspects of the bill collection process, is completely safe, and uses viral evolution to adaptively improve its performance over time.

The stupid claim that holding a contest to write benevolent virus applications is somehow related to the HIV analogy demonstrates Jim's tunnel vision. It is the same tunnel vision that prompted much of the security community to ignore my work on virus defenses until viruses became such a big issue that they began to embrace my results and use my defensive techniques. The computer virus contest is not a bomb making competition, and only a half-wit or someone with a commercial interest in keeping his customers afraid could have derived that interpretation from the facts surrounding the contest. The idea that we should live in fear only profits those who sell the antidote for fear, and their tool for instilling fear is propaganda and ignorance.

Mr. Bates is certainly not connected with *Advanced Systems Protection*, which has provided computer integrity protection products, services and education since 1985. I doubt whether we would seriously consider his application and we certainly do not endorse his brand of scare tactics or peddling of ignorance for profit.

Sincerely yours,

Dr. Frederick B. Cohen
President - ASP
Pittsburgh, Pennsylvania, USA

Editor's reply

Jim Bates is currently lecturing in the United States but will be granted the usual right of reply to this letter next month. With regard to Dr.Cohen's assertions about Virus Bulletin, they are some points he makes which need correcting:

1. *As an erstwhile member of VB's editorial board, Dr. Cohen must know that his assumption that Jim Bates' opinions reflect 'the official views of Virus Bulletin' is incorrect. There are currently twenty editorial advisors to VB, all of whom reflect their own opinions.*
2. *Neither Virus Bulletin, its editorial board, or any of its writers stated or implied that Dr. Cohen or Advanced Systems Protection published virus source code.*
3. *Dr. Cohen states that VB 'refused' to review his Integrity Toolkit. VB's evaluators never refused to review this product - they were simply unaware of its existence prior to receipt of the above communication.*

From 'Ports of Trade'

To Be Published in Full or Not At All

We would like to express our gratitude to *Virus Bulletin* and Dr. Keith Jackson for the evaluation(s) performed on *Viruguard*. Not only did they point out some minor problems [1] and desirable enhancements, which the developers were quickly able to amend and implement [2], the evaluation exercise reaffirmed our belief that *Viruguard* is an extremely effective anti-virus tool [3].

The results in which was claimed that 93% of the viruses tested were detected, are inconclusive [4]. Some of the twelve viruses that apparently were 'not found' by the card during your test are in circulation in South Africa, and are detected and stopped by *Viruguard*. This indicated that the viruses used during the test were possibly:

- not active during the test period

- not attempting to replicate at any stage during the test period

- were not loaded before or during the test period [5]

The evaluator confirmed telephonically that the twelve viruses 'not found' by the card could not be detected anywhere in his computer after the test. This fact was not reported [6]. *Viruguard* only alerts the user when a virus attempts to activate. The tests conducted did not prove that any virus operated without being detected by the *Viruguard* during the test period [7].

The benchmark test conducted by independent evaluators appointed by the developers show very different results from those published by *Virus Bulletin*. These tests were conducted using *PC Magazine's* Benchmark Tests Version 5.5. The results are available on request [8]. *Virus Bulletin* has not stated which benchmark tests were used [9].

Robbie de Clercq
Ports of Trade
Cape Town, South Africa

The Evaluator's Reply:

This apparently resonable letter is in fact a tissue of of misinformation, half-truths and distortion and as such demands a very firm reply.

[1] I pointed out some serious omissions, not minor errors. The details are contained in the review.

[2] The statement that developers were able to amend things quickly is a joke. Two *ViruGuard* cards had to be sent as the first one did not work properly on my test computer. A replacement disk supposedly containing software upgrades actually contained a second copy of the original files. The promised amended documentation (a new README file) never did arrive. I could go on...

[3] The vendors may believe that *ViruGuard* is an extremely effective anti-virus tool but my review findings suggest differently. I do not wish to restate my opinions; let the review speak for itself. I stand by every single word.

[4] The results are not 'inconclusive', they are quite clear. *ViruGuard* failed to detect some virus infected files which were executed when the *ViruGuard* card was present. Period.

[5] I can repeat such tests ad infinitum. If the product was to be returned in the state it was in before, it would still fail to detect these viruses. It would fail to detect the viruses no matter who did the test. This matter should not even be in dispute, it should be patently obvious.

[6] It was not reported because IT IS NOT TRUE! I am *staggered* by this attempt to put words into my mouth.

[7] The tests showed that some virus infected files could execute on a computer with the *ViruGuard* card present. The rest is weasel words provided by the vendor of *ViruGuard*.

[8] I cannot speak for *PC magazine*. I simply re-iterate that using my standard virus test set, *ViruGuard* failed to detect a specific sample of these viruses. The results are closely documented in my review. They are repeatable.

[9] Not true. The *Technical* Details section at the end of a *VB* review lists viruses that are used for testing. It states how many strains of each virus are used for testing, and describes the hardware on which the tests are carried out.

As the developer has seen fit to reply with such a distorted, error-ridden letter, I feel obliged to add a few general points about the review, and provide a bit of background information as to what happened, as not all the facts about what went on while this review was being written have been published. Put simply, I feel that the review was in fact *kind* to *ViruGuard*.

After the first version of my review was read by the vendors of the *ViruGuard* hardware, *VB* received a written communication demanding that it not be published. This threat was only removed after the developers phoned me, three times, and I refused to discuss matters until the insinuation of legal restraint was removed (in writing).

I really do feel that the vendors of this product have abused *VB's* review process. I spent more than twice as long reviewing this one product than any other product in the whole of *VB's* three-year history. Weeks later, I'm *still* writing about it. I partook of over half a dozen, long, phone calls to South Africa (at their expense), to help explain the problems, and suggest solutions. At times I felt as if I was providing unpaid consultancy to the developers of *ViruGuard*. Acting as a free development service is not *VB's* function, and as *VB* reviewers are paid by the word, I earn nothing extra from providing such telephone support.

Trying blindly to quote other (more favourable) reviews is merely an intentional attempt to mislead people. *VB* was absolutely deluged by such material about *ViruGuard*. I have on my desk at this moment a 26-page fax, a 23-page fax, and a 29-page fax. All providing reams and reams of test results from *ViruGuard's* developers which are meant to somehow 'prove' that *ViruGuard* is 'perfect' at detecting viruses. I cannot for the life of me see what I gain from them, apart from the knowledge that their own results are different. I say it again, I stand by every word in my review. I chose my words in the review with great care. If the fax deluge was an attempt to shut me up, it has had the opposite effect.

VB reviews products exactly as they are received. If the product isn't fully tested, don't ship it to *VB* for review. To help the developers of *ViruGuard*, I even broke a long standing rule that products do not come back for retesting immediately after being 'amended' (their word), and I arranged that *VB* would provide a second part for this review. This was done in the interests of fairness. Frankly I now wish that *VB* had not bothered to do this.

Those who read *VB* regularly will know that I rarely reply to comments on my reviews, apart from pointing out obvious errors of fact. People have a right to comment on what I say in a review, and they should be allowed to put their thoughts in print without let or hindrance. However, this whole experience with *ViruGuard* has so shocked me that this one time I just had to reply in detail.

To reiterate a quote that I have used before: The vendors are trying to sell their product. I am trying to produce an objective assessment of the product. I let the readers of *VB* make up their own minds about where truth is likely to reside.

Keith Jackson

From S&S International

With reference to your review of *ViruGuard* in the February 1992 issue of *Virus Bulletin*, *S&S International* would like to point out that *ViruGuard*, despite the similarity in name, is in no way related or otherwise connected with the *VirusGuard* TSR virus blocker program in *Dr. Solomon's Anti-Virus Toolkit*. The name *Dr. Solomon's VirusGuard* is a registered trademark of *S&S International Ltd*.

Thank you for the opportunity to point this out to your readers.

Pat Bitton
Marketing Consultant

From XTree Company

Dear Mr. Wilding,

We were quite disturbed by your review of *ViruSafe* and *Allsafe* in the January 1992 edition of *Virus Bulletin* as it contains information which we find incorrect.

We fail to understand why Mr. Hamilton chose to make an issue of our taking the reference to copy protection out of the quote by Dr. Keith Jackson. Mr. Hamilton seems to imply that we dishonestly changed the quote, when we simply removed reference to copy-protection which no longer applies to *ViruSafe* and in no way changed the spirit of the quote, which praised the product.

VC is much smarter than the review implies. There is a problem with encrypted viruses that have a meaningless signature. However, of the 1200 known viruses, only about 30 are encrypted.

New encrypted viruses are added to the *ViruSafe* software via hard coding, as is done by other manufacturers. Mr. Hamilton is wrong when he states that our software does not take this approach. By the way, the pattern automatically chosen [*from non-encrypting virus code*. *Ed*.] is not the first byte. There is a very smart built-in algorithm that carefully selects where in the file to begin checking for unique signature patterns.

There is a fundamental mistake in Mr. Hamilton's discussion of the fact that *UnVirus* found 431 viruses in 324 files. In the slow mode (which was apparently used) we show the viruses and possible mutations found in an infected file. This is documented in the *ViruSafe* manual on page 38. This option can be disabled. Thus the removal capabilities cannot be called into question. During removal of a virus, we carefully check that this is indeed the virus we intend to remove.

Thanks in advance for printing this clarification.

[Illegible signature]

XTree Company, Obispo,
California, USA

Editor's reply

XTree deserves a formal apology. Normally reviews are sent to manufacturers prior to publication so that legitimate points, such as those raised in this letter, can be incorporated into the text. Unfortunately, in the case of XTree's ViruSafe, the Christmas recess interfered with this process.

The only claim in this letter which the evaluator questions is the statement that VC contains a 'sophisticated algorithm' which can automatically select search patterns for unknown viruses. In extensive testing with a large number of unencrypted viruses there was no evidence to suggest that this was the case, the program invariably selected the first 16 bytes of virus code.

TECHNICAL SUPPORT

Writer: Mark Hamilton

Researcher: Vanessa Burridge

The Call of Duty

Following last month's survey of 'out-of-hours' technical support, VB continues its enquiry this month with an assessment of the quality of 'office hours' support provided by the prominent anti-virus software houses.

New Zealand 2 is the most prevalent computer virus which, according to those organisations which log reports, accounts for 30 to 50 percent of all virus incidents reported. Accordingly, anti-virus software developers should have intimate knowledge of this virus and be able to render assistance in clearing it from infected PCs. *VB's* researcher contacted the technical support departments of the anti-virus companies. She told each in turn that she had detected the New Zealand 2 virus on a hard disk using the current version of their product.

In addition to the anti-virus software developers there are other agencies which provide advice to users: *Scotland Yard's Computer Crime Unit*, the *National Computing Centre* (UK) and *NCSA* (USA). To forestall the possibility that these agencies would simply refer her to the package's author, she told them that she had discovered the virus using Fridrik Skulason's *F-Prot* (*VB's* technical editor's software).

In all cases, her call commenced with the explanation:

> *Hello, my name is Vanessa Burridge. I work for an independent financial adviser. I have just started scanning our PCs and have discovered that one of them has [New Zealand 2 / Stoned] on it. We have two other PCs but these haven't been checked yet, what shall I do?*

The nomenclature used for the virus matched that used by the relevant anti-virus package. Her findings are reproduced in full and are followed by an verdict based on *VB* evaluators' experience of the package concerned. A model answer from technical support operating in the UK should include mention of the importance of reporting the incident to the police.

Metropolitan & City Police Force Computer Crime Unit

✆	071 230 1176
Time:	11.10am, Thursday 12th March 1992
Contact:	Detective Sergeant Barry Donovan

Researcher's Report

DS Donovan told me that I must check the other two PCs and he asked me if it was the software telling me the virus is present rather than the virus announcing itself. 'This is a Friday the 13th virus', he said. At this point Donovan consulted someone else in the office and I heard the word 'Stoned' mentioned - I took this to be a reference to the virus, not the *CCU*! Donovan returned to the phone saying, 'I'm sorry, I'm wrong. This virus is actually a derivative of the New Zealand virus. I suggest you contact a Mr. Bates on 0533 883490 - he is a virus specialist and one of our consultants. Once you've spoken to him perhaps you'll get back to us and let us know how you've got on.' I did not call him back.

Verdict:

The *CCU* routinely recommends specialists to callers based on the simple criteria that the researcher will assist the caller as fully as possible free of charge. Despite an initial and quickly corrected mistake, the *CCU* rightly identified the virus as being a derivative of the original New Zealand virus and referred the researcher to a specialist. As a postscript, the police filed this call and sent a report to its statistics branch at Scotland Yard. The police have subsequently been informed of this investigative exercise and *VB* apologises for wasting police time.

Bates Associates

✆	0533 883490
Time:	11.25am, Thursday 12th March 1992
Contact:	Answerphone/Jim Bates

Researcher's Report

The phone was answered by a machine and I left the message 'I've been told by DS Donovan of the *CCU* to contact you as I've discovered New Zealand 2 on one of my PCs'. Jim Bates called back at 1.50pm and said, 'New Zealand 1 and 2 are very different. Yes you must check the other two PCs.' At this point he asked me what version of *F-Prot* I was running and I said 2.2. 'That is one of the older ones but in my opinion, it is one of the better ones. Boot the machine by using the original disk that came with it - this disk should be clean and write-protected. Boot from this and then scan again. If New Zealand 2 is there it will be in the Master Boot Record on track 0, head 0 and sector 1.' I mentioned that I had a copy of *The Norton Utilities* version 4.5 and he suggested that I use this to look at the disk. 'If the virus is on track 0, head 0, sector 1, it will have stored the original Master Boot Record on track 0, head 0, sector 7. If nothing is recognisable on sector 7 then look at sector 2. Then the virus is on sector 1. Collect sector 7 and put it on to sector 1. Use *The Norton Utilities* and view track 0, head 0, sector 7 using the menu. The screen will show what looks like garbage, plain-text error messages and at the bottom of the screen - about one-third of the way up from the bottom, it will be mainly zeros. When it is recognisable as the Master Boot Record, then press Escape and tell it you want to write sector 7, in absolute mode, to sector 1. Once it has done this, it's then destroyed the virus and restored the machine.'

Verdict

A flawless disinfection of the hard disk. Jim Bates cleared New Zealand 2 using 'traditional' tools. This method is perfectly acceptable and is effective. The reason he mentioned sector 2 is that the earlier strain of this virus (New Zealand 1) stores the original copy of the Master Boot Sector there. Since, from a scanning point of view, the two viruses are very similar - and some scanners may not differentiate between them - Jim Bates was taking the cautious approach. However, no mention was made of checking and clearing diskettes.

The National Computing Centre (NCC)

✆	061 228 6333
Time:	11.40am, Thursday 12th March 1992
Contact:	Chris Hook

Researcher's Report

He told me to 'check the other two PCs. There has obviously been an interchange of disks, so it's important to check any other machines you have.' He asked me if we had any backup copies of data. He said that he didn't know *F-Prot*: 'I'm afraid I don't know all the packages on the market but provided the software tracking virus package has been regularly updated, it should detect any virus. If it's on the other machines then check all the disks. This is disruptive to work schedules but well worth the time.'

I then asked him if there was an antidote. 'This depends on the package you have', he said. 'Once you've located which machines have the virus, then contact the company you purchased the package from. Some packages try to erase the virus, otherwise you'll have to reformat - that's why backup disks are so important.'

Verdict

The *NCC* does not profess virus expertise, nevertheless Mr. Hook provided sound, practical advice. Significantly, he stressed the importance of backups. Regular backups are a very important aspect of fighting computer viruses and can be a life-saver. He also discussed the vital importance of checking diskettes. However, there was no mention of reporting the incident to the police.

NCSA Inc., USA

✆ 0101 202 364 8252
Time: 2.25pm (EST), Thursday 12th March 1992
Contact: Answerphone

Researcher's Report

The answerphone said, 'You have reached the *National Computer Security Association*. We are not in on March 12th or 13th but you can leave a message.'

Verdict

NCSA's directors were attending the *Fifth Annual Computer Virus & Security Conference* in New York. Given its high profile one might assume that *NCSA* would provide at least one person to take calls, particularly on a Friday 13th!

RG Software Inc., USA

✆ 0101 602 423 8000
Product: *Vi-Spy* version 8
Time: 1.40pm (CMT), Thursday 12th March 1992
Contact: David Lee

Researcher's Report

I was asked for the company name and my name for the records, which I provided. When I asked him if I should check the other two PCs, Mr. Lee asked me if *Vi-Spy* had been installed previous to the infection. He said, 'Turn-off the PC and boot the machine from a clean system disk. Put *Vi-Spy* into the C drive and issue the command VI-SPY C:/NF. Then it tells you the infection is there but should not find the virus in memory, only in the partition sector. Go back to the C prompt, type VSRECOVR A: C: (have a diskette in the A drive at this point) and it will remove the virus from C disk. It will then ask you questions - you must answer all these with a 'Yes' otherwise it will stop working and will not clear the virus. It will ask you if you want to recover - you say 'Yes'. The virus should now be removed.'

Verdict

David Lee provided clear instructions on how to remove the virus using *RG Software's* in-built boot sector recovery routine. A near-faultless reply marred by the fact that Mr. Lee did not mention the importance of checking diskettes.

X-Tree Company

✆ 0101 805 541 0604
Product: *Allsafe* version 4.54
Time: 1pm (PST), Thursday 12th March 1992
Contact: Mark

Researcher's Report

An answerphone gave the message, 'Thank you for calling the *X-Tree Company*. For technical support and removal of the Michelangelo virus press 2 .....' I was then connected to the main reception and I asked for technical support where I spoke to Mark. He had just got back from lunch and commented that I was working late (it was 9pm in London). He checked his records for some time. He asked for my name (but not my company's name) and he apologised for the wait, saying he was pulling all the information he could find on the virus. 'Right', he said, 'here we are now. New Zealand 2 is a very common virus. Here in the USA we call it the 'Stoned Marijuana' virus and it is in the boot sector of the hard drive. If your PC is on, it is always in the memory. Get a floppy diskette, one that came with the PC that is write-protected, and boot of the floppy diskette. 'Go to the *Allsafe* directory and type in *UNVIRUS*. It then shows you the menu. Tell it to check the boot sector and to check C drive. The screen flashes and says 'Found and removed NZ2 or SMV'. Then take the disk out and immediately re-boot the PC. You have at least one infected floppy disk that you have booted off, so check all the disks before re-inserting them.' Mark was very helpful and told me to ring back if I had any problems.

Verdict

X-Tree users outside the United States have to call the company in California to get technical support. Mark knew his stuff and provided clear and correct directions to remove the virus. He also advised checking all floppy disks for the virus.

International Data Security Ltd.

✆ 071 631 0584
Product: *McAfee Associates' Scan* version 85
Time: 12.10pm, Friday 13th March 1992
Contact: Oliver Mills

Researcher's Report

IDS is the UK agent for *McAfee Associates*' products. I had to hold the line for five minutes as lines were busy in the technical support department. Mr. Mills took the call and said, 'Yes it is worth checking the other two PCs. We are moving

offices today so my PC is down. Use a McAfee write-protected disk so that it doesn't get infected and this should be able to clean the virus. The tools are on the write-protected McAfee disk - plus the DOS disk - and you should be okay with these. 'If you have any problems, please phone again.'

Verdict

One can only assume that the change in offices partly accounted for the cursory advice proffered by *IDS*. But it should not have been necessary for *IDS* to consult any PC virus database in order to be able to instruct users on the correct procedure for removing this the most common of all viruses. When you consider that McAfee's software clears this virus with consummate ease (see below), *IDS* should know the products it sells and supports sufficiently well to pass on the brief, relevant instructions.

S&S International Ltd.

☎ 0442 877877
Product: *Dr. Solomon's Anti-Virus Toolkit* version 5.54
Time: 12.21pm, Friday 13th March 1992
Contact: David Emm

Researcher's Report

Mr. Emm said, 'This is in fact the Stoned virus. The infection has to be on a floppy disk for the hard disk to be infected. The disk will infect through the A drive when you boot the machine. If the machine is infected, it will infect any disk in drive A that is inserted.

Boot the PC from a clean DOS disk. When the A: prompt shows, put the *Toolkit* (3.5 inch disk) in and type *UNSTONE*. This is the program on the *Toolkit* that is designed to clean the virus from the hard disk. It will clean up Stoned. Run *FINDVIRUS* again to confirm that machine is clean. Use the same procedure for the other two PCs: run *FINDVIRUS* first then *UNSTONE* to clean. 'For the floppy disks - if they are all labelled, gather them together and use *FINDVIRUS* to tell if the floppy disks are infected. Give disk drive as A when you run it and examine the first floppy, then press drive letter and keep feeding the disks in. It will take time but should tell you which ones are infected. The program to clean the Stoned virus off floppy disks is *CLEANBOOT*. This lets you feed in disk after disk. The floppies are important because they can re-infect the machine.'

Verdict

A faultless technical reply marred by the single fact that no mention was made of reporting this incident to the *Computer Crime Unit*.

Total Control (UK) Ltd.

☎ 0488 685299
Product: *VIS Anti-Virus Utilities* version 3.33
Time: 12.35pm and 12.45pm, Friday 13th March 1992
Contact: Unknown

Researcher's Report

On my first call I was asked by the receptionist to hold the line. Then she came back and asked me which virus it was and said someone else could probably help as technical support were busy on the telephones. This 'someone else' was not there so she asked me to call again in five minutes. When I called back, a different woman answered the phone. When I told her the problem she said she would probably be able to help. She said it was worth scanning the other two PCs. 'Use *VISCHECK* and refer to the manual - it will tell you how to run it.' I rather got the feeling, from the tone of her voice, that they were too busy to help me. I never did get through to technical support.

Verdict

Total Control should have taken our researcher's number and got the technical support department to call her back. The program our researcher was asked to run does not clear boot sector viruses, it is a generic file checker. Since *VIS* users do not normally have access to the program's author (Jim Bates), it is *Total Control's* responsibility to provide technical support. This is hardly a creditable performance.

Symantec UK Ltd.

☎ 0628 776343
Product: *Norton Anti-Virus* Version 1.5
Time: 12.50pm, Friday 13th March 1992
Contact: Rob

Researcher's Report

Lines were busy when I rang, so I was asked to hold and five minutes later, Rob took the call. 'Boot from a clean floppy disk (a MS-DOS disk) - this makes sure that no virus is in memory - and load *Norton Anti-Virus* by typing NAV, it then shows the program. Scan the hard disk and it finds the virus. If it tells you that it is reparable, then use the 'Repair' button. If not then use the 'Delete' option on that file. The manual actually explains the whole system. 'Yes, do check the other two machines. If you have any problems, just phone back and ask for me, Rob, or for Jamie.

Verdict

The fact that *Norton Anti-Virus* does repair New Zealand 2 infections means that this advice successfully cleared the machine. However, Rob should have known that New Zealand 2 (or Stoned) is a boot sector virus and not a file virus, so the 'Delete' option is hardly appropriate. He failed to point out the importance of scanning floppy disks. No mention was made of reporting the incident to the *Computer Crime Unit*.

Sophos Ltd.

☎ 0235 559933
Product: *Sweep* March 1992 Edition
Time: 1.05pm, Friday 13th March 1992
Person: Richard Jacobs

Researcher's report:

I was immediately put through to Mr. Jacobs who, after I explained my predicament, said, 'Yes do check the other two PCs. This is a boot sector virus that has gone in right at the beginning. You should use the *SU* program of *Sophos' Sweep*. I can fax you through all the details now if you like.' I asked him to give verbal instructions as I didn't have a fax machine.

'Run SU with the command line: SU -WR C: which starts SU. The virus is in the first sector. From SU's main menu, select option 1, 'View Item', then option 1, 'Absolute Sector', and reply with head 0, cylinder 0 and sector 7. It then displays the contents of the sector on screen. It will display a load of junk numbers in the right-hand column - text 'Invalid Partition Record'. On the left hand part of the screen, at the bottom, the last two numbers should be 55AA - these are hex numbers. 'Press enter and it gives you the original menu. Use option 5 from the main menu, select option 2 - 'Copy Item' - and then option 1 - 'Absolute Sectors'. Give head as 0, cylinder 0, sector 7 and number of sectors as 1. If you're not in at this point, press enter. Select 'Destination Item', choose option 1 - 'Absolute Sectors' - and give head 0, cylinder 0, sector 1. SU then warns you to confirm that you want to go ahead. Select option 2 and it then removes the virus. 'At the beginning, don't forget to turn the PC off and to boot it from a clean DOS disk - one that is write-protected.' He then told me that these virus incidents were illegal and suggested I report finding the virus to the *CCU* and that I should quote reference number SOP92378.

Verdict

A flawless talk-though on removing the New Zealand 2 virus using the *Sophos Utilities* program. This was the only company to point out the legal situation pertaining to viruses and the only company to suggest that the incident be reported to the police. A first-class response marred by the fact no mention was made of the importance of checking diskettes.

Frisk Software (Iceland)

☎ 010 354 169 4749
Product: *F-Prot* version 2.2
Time: 12.25am (local), Friday 13th March 1992
Contact: Receptionist

Researcher's Report

I was told that the author, who answers all technical questions himself, was away in New York until the following Monday.

Verdict

Fridrik Skulason was attending the aforementioned 'Ides of March' computer virus conference when our researcher called. Unfortunately, viruses do not respect researchers' busy schedules and this illustrates one of the problems inherent with small companies.

Fifth Generation Systems UK Ltd.

☎ 0494 442224
Product: *Untouchable* version 1
Time: 1.40pm, Friday 13th March 1992
Contact: Trevor Jones

Reviewer's Report

I had to hold on for several minutes before speaking to Trevor Jones, in the company's technical department. 'Refer to the *Untouchable* manual', he said. 'Boot the machine and it does a check. It then displays the virus and asks you whether you want to remove it or ignore it. Tell it you want to recover. It doesn't just detect the virus, it recovers it too. You may need to put a safe diskette in.' 'I asked him about the other two PCs and he answered, 'if *Untouchable* is installed on the other two machines check them. Your PC should tell you which file the virus is on - if this infected file is on the other two machines you can remove that file straight away and clean it on the original PC.'

Verdict

Mr. Jones' obvious lack of virus knowledge is apparent - New Zealand 2 is not a file virus. He makes the assumption that no one has tinkered with the PC's startup files (CONFIG.SYS and AUTOEXEC.BAT) which cause *Untouchable* to run on each reboot. Never assume anything where users are concerned! There was no mention of checking diskettes and no mention of reporting the incident to the police. However, despite the inadequate advice given *Untouchable* did recover the hard disk due to its in-built disinfection routine.

VB Software (Ireland)

☎ 010 353 627 5404
Product: *Virus Buster*
Time: 2.20pm, Friday 13th March 1992
Contact: Alan Lowe

Researcher's Report

Mr. Lowe asked me to tell him the serial number of the anti-virus software which was on the top, right-hand corner of the disk. I declined to provide the serial number. He flatly refused to provide information without the serial number and instead asked me for my name and phone number.

Verdict

VB Software is in the process of setting up *Leprechaun Software UK* which will provide technical support for the United Kingdom. A good-natured letter from Managing Director Jack Kenyon explaining this development arrived too late for publication in this issue.

Microcom (European Office)

☎ 010 331 466 26868
Product: *Virex-PC* version 1.8
Time: 3.30pm (local), Friday 13th March 1992
Contact: Friska

Researcher's Report

The technician was away. Friska referred me to the Woking office (see below) and suggested I talk to Nigel.

Verdict

Microcom's Woking number is not published in its manual.

Microcom (UK)

☎ 0483 740763
Product: *Virex-PC* version 1.8
Time: 2.35pm and 3.30pm Friday 13th March
Contact: David Free

Researcher's Report

I asked for Nigel but was told he was away on holiday until Monday. I asked if anyone else in technical support could help me and was told that David Free could, but he was on the telephone so would I leave my name and number and he would call me back. At 3.30pm, I had not been called back, so I rang again and was told that David Free was still tied up on the phone. David Free returned my calls at 4.30pm. 'If the machine has found the virus, it should be able to repair it. The USA office really handles viruses.'

He suggested that someone else from his office may be able to help me, but he would have to get them to ring me back later. I asked him whether it would be quicker for me to phone the States - 'Much quicker', he replied. 'They are only five hours behind us so you could ring them now. The number is 919 490 1277 and ask for *Virex* support. Some of them may be at lunch now, though.'

Verdict

It is not unreasonable to expect a company marketing anti-virus products to have a modicum of knowledge about the most prevalent viruses and how to deal with them. Microcom's UK office appears to have no such knowledge.

Microcom (US)

☎ 0101 919 490 1277
Product: *Virex-PC* version 1.8
Time: 3.35pm (EST), Friday 13th March 1992
Contact: Gary

Reviewer's Report

I was asked to hold the line until someone was free to assist me. Seven minutes later, Gary came on the line and said, 'The shareware package is 1.8. This virus is called the Stoned virus here in the US and it's a boot sector virus. You really need to buy the commercial product from *Microcom* in your country or you can low-level reformat the hard drive to remove the virus. This rebuilds the partition table and the boot sector but it can reinfect. 'I suggest you buy the new commercial copy of *Virex-PC* in the morning. Stoned does not format the drive or kill files, but probably most of the disks and the hard drive are infected. You should have a back-up of the hard drive.' He was unable to do more to help me.

Verdict

The product referred to above was supplied to *Virus Bulletin* by *Microcom* (US) and is not a shareware version. Quite why the researcher should have to buy a second copy of the product is not clear.

Low-level formatting is not a perfect solution: it does not, as Gary stated, rebuild the partition table or the boot sector. The virus can be cured by far more elegant means as other vendors

have demonstrated. The researcher had to make four calls to three *Microcom* offices in as many countries, only to be told to buy another copy of the product.

Fifth Generation Systems Inc. (US)

✆	0101 504 291 7221
Product:	*Untouchable* version 1
Time:	3.50pm (EST), Friday 13th March 1992
Contact:	Kirk

Researcher's Report

'Select the option to remove the virus. If the virus has been there for a while, the master boot record could be damaged. Get a full files-only back-up. Put *UTSCAN* against it, if it's giving you the option. 'Run *UTSCAN* against the hard disk. Once it has removed the virus, re-boot the PC and install *Untouchable*. Get the memory and boot sector clean and then run the Install program. *Untouchable* should have no problem erasing the virus.'

Verdict

Kirk gave sounder (and more correct) advice than his UK-based counterpart. But he failed to mention the importance of cold-booting the PC using a clean, write-protected DOS disk and the equal importance of scanning all floppy disks.

Central Point Software Inc.

✆	0101 503 690 8088
Product:	*Central Point Anti-Virus* version 1.1
Time:	1.05pm and 2pm (PST), Friday 13th March 1992
Contact:	Receptionist, messaging system and answerphone

Reviewer's Report

When I got through, I was told, 'We are having problems with our technical support department and they probably won't be able to get back to you until Monday. However, we are open for another five hours, so please call back when someone may be able to help you.' I said that I couldn't leave it until Monday and that I'd call back in an hour. At 10pm (GMT) I called again - and was asked to hold for a moment. The receptionist then answered and I requested technical support. She put me through to a messaging system which gave me nine different options - which took what seemed like several minutes to detail. Option 2 was for technical support, so I pressed '2' on my phone and got an answerphone which asked me to hold - 'but this could be for some time. If you hold more than five minutes, you can then leave a message or you may use our fax facilities.' I hung up, with frustration.

Verdict

Judging from messages left by *Central Point* users in *Compuserve's Virus Forum* over the last few weeks, the researcher is by no means alone: her disillusioned view of *Central Point's* technical support is shared by quite a few other 'real' users.

Central Point Software International Ltd. (UK)

✆	081 569 3316
Product:	*Central Point Anti-Virus* version 1.1
Time:	1.45pm, 1.55pm, 3.35pm, 16th March 1992
Contact:	Linda and company answerphones

Reviewer's Report

'Hello, you are through to the technical support hotline. Your call is held in a queue for up to a maximum of three minutes. We apologise for the delay in taking your call, this is due to the demand on the Michelangelo virus.' The machine then went on to give me a lot of company information.

When Linda eventually came on the line, she asked me to check whether the version was 1.1 or 1.2 and the date of the files. She then explained, 'the date of the file will confirm whether or not we can clean the virus.' I said I would check and phone her straight back. In fact, the files are dated 22/08/91 and timed 13.10 (meaning version 1.1).

I rang back (at 1.55pm). After holding for three minutes (to the tones of Vivaldi's *Four Seasons*), I left a message for Linda on the answerphone. As Linda had not called in the interim, I called the company again at 3.35pm. I held for another three minutes, got bored with the *Four Seasons*, and left yet another message for Linda. By 5.25pm, I still had not received a call from Linda - or anyone else from the technical support team. If I was a real client of theirs, I would certainly not be buying any further software from them. After all, I have made five phone calls to this company (including the two to the States) and received no satisfaction whatsoever. How busy can the London office be with Michelangelo? I really feel angry on behalf of their customers.

Verdict

You shall be taken from this court to a place of lawful execution...

McAfee Associates Inc. (US)

✆ 0101 408 988 3832
Product: *Scan* version 85
Time: 3.55pm (PST), Monday 16th March 1992
Contact: Receptionist, Aryeh Goretsky

Reviewer's Report

The receptionist who answered the phone asked me if I had tried cleaning the disk yet? I replied that I had not as I'd got two other PCs in the office and didn't know whether to touch them because of the virus. She warned me that technical support were very tied up - but as soon as she'd said this, Aryeh Goretsky came on the line. 'Can I just confirm which *Scan* version you are using - the one that located the viruses', he asked. I told him I was using *Scan* version 85. 'Right, well, to remove the virus, first turn-off the PC and boot off a clean copy of DOS, such as the original diskette, and run the virus *Scan* program against the boot disk, just to make sure it's virus-free. 'Back-up the hard disk as a precaution. Run the *CLEAN* program - type CLEAN C: [STONED] and press enter. It runs for 10 or 20 seconds. Reboot off the DOS diskette and re-run *Scan* to confirm the virus has been removed. 'Use *Scan* to check any floppies in the A drive that may have been infected.'

Verdict

A first-class response.

Limitations and Bias

All the calls were made during the normal business hours of the company called, therefore there was no bias in favour of any one supplier or group of suppliers.

Conclusions

This survey highlights that, in general, the smaller, specialist companies provide a higher level of technical expertise than those companies where anti-virus products are one constituent of a larger product portfolio. It is interesting to compare these results with those in the *VB* comparative reviews of scanner performance, where, again, the specialist companies win through. Plaudits are due to *Bates Associates*, *RG Software*, *X-Tree*, *S&S*, *Sophos*, *McAfee Associates* and *Fifth Generation Systems* (US), for providing sufficient and in some instances, excellent, technical support. This survey will be repeated.

Editor's Statement

This survey was conducted with the prior knowledge of *the editor, the author of this report* and *the researcher* who conducted the survey. No other person or organisation had prior knowledge that this survey was being conducted.

PRODUCT UPDATE

Keith Jackson

Norton Anti-Virus Version 2.0

Norton Anti-Virus has been reviewed before in *Virus Bulletin* (*VB*, January 1991), but as v2.0 has now been released (a major upgrade), it seemed time for *VB* to have another look. For reasons best known to themselves (I refuse to speculate on their motives), the UK vendors of *Norton Anti-Virus* were not willing to provide a review copy in the normal manner, therefore the copy of *Norton Anti-Virus* discussed in this review was actually purchased by myself as a normal user.

I bought my copy of *Norton Anti-Virus* v2.0 in early March 1992, and the latest files on the disks were dated 21st December 91. In the same week that my copy of v2.0 arrived, *VB* received (unannounced) an upgrade for the copy of *Norton Anti-Virus* reviewed in January 1991, which contained files dated variously between 5th August 1991, and 25th February 1992. Some of the files on the upgrade disk were actually older than the files on my 'real' version (by four whole months!), yet the virus definition files on the upgrade disk were dated 25th February 1992, two weeks before I placed the order for *Norton Anti-Virus* with *Symantec*. There seems to be a failure of version control here, not to mention a failure of communication. An inauspicious start.

I used *Norton Anti-Virus* v2.0 as purchased, but upgraded this to include the 25th February 1992 virus definitions.

Installation

The install program provided with *Norton Anti-Virus* is easy to use, and warns clearly against installation on a computer already infected by a virus. It offers to scan the hard disk to check that a virus is not already present. Inoculation files used by previous versions of *Norton Anti-Virus* can be removed by the installation process, and *Norton Anti-Virus* v2.0 can be installed either for DOS, or for *Windows 3*, or both. In the latter case just over 1 Mbyte of storage space is required on the hard disk.

The installation process requires that you enter your name to 'personalise' the copy of *Norton Anti-Virus* (a form of copy protection that I find acceptable), choose which type of device driver is to be used by *Norton Anti-Virus*, and decide where the *Norton Anti-Virus* files should be stored. A user is also given the opportunity of creating a 'rescue' disk containing information about the Master Boot Sector and DOS Boot Sector of the hard disk. *Norton Anti-Virus* can restore this information back should anything go disastrously wrong at some future date. I can't fault the installation program.

Version 2.0 of *Norton Anti-Virus* claimed to know about 340 unique viruses, spread across 1005 virus samples. The upgrade disk for v2.0 increased this total to 341 viruses, of which there were 1006 unique samples.

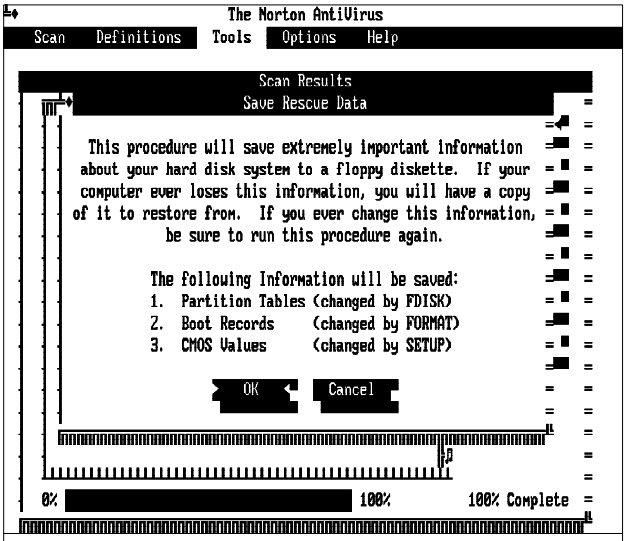
The last time that *Norton Anti-Virus* was reviewed, it knew about 115 uniquely named viruses, with variants increasing this total to 142. How things have moved on in just 15 months. The upgrade process stated that it was providing definitions (signatures) for 30 viruses, and most of these were merely upgrades. Whether they were provided because the old signatures were faulty was not made clear.

Documentation

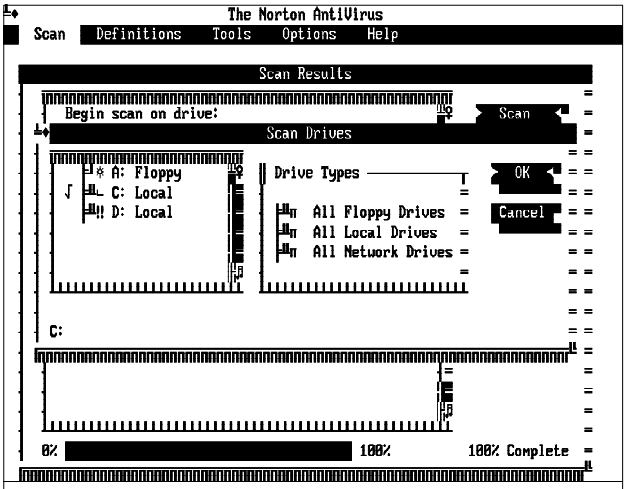
In its original guise (*VB*, January 1991), I was highly critical about the documentation that came with *Norton Anti-Virus*. This was primitive to the extent that most of the interesting points (including all the error messages), were not even mentioned in the manual, they only appeared in one enormous README file. I'm pleased to see that this has changed.

Norton Anti-Virus now comes with three manuals: an installation booklet, an A5 manual explaining execution under DOS, and an A5 manual explaining execution under *Windows*. These are all well written, indexed, and easy to use.

The DOS and *Windows* versions of *Norton Anti-Virus* are remarkably similar. In fact apart from the unique *Windows* graphical style, anyone would be hard pushed to design them to be any closer. There is of course a third possible method of operation, which is to execute the DOS version from a DOS box within *Windows*. I'll discuss all three.



Creating a 'safe disk'. Making backups of boot sectors and Partition Tables is now recommended practice - *Norton Anti-Virus* simplifies this process.



The fixed disk is selcted for scanning. *Norton Anti-Virus* is 'network aware' being compatible with *NetWare*, *Lan Manager* and *3COMM*.

Operation

Norton Anti-Virus comprises two main components: *Virus Clinic* and *Virus Intercept*. *Virus Clinic* is a stand-alone program that can scan for the presence of viruses, inoculate files, repair files, in fact a whole host of functions. *Virus Intercept* uses a device driver that performs various tests while the operating system is in use.

Scanning

Both the DOS version and the *Windows* version perform a test scan when *Virus Clinic* is loaded (see below). In line with most scanner programs, *Norton Anti-Virus* scans memory for viruses before it tests the hard disk. This memory test took 9 seconds under DOS, and 5 minutes 6 seconds under *Windows* (thirty-four times slower!).

The actual scan of the hard disk took 1 minute 24 seconds under DOS, and 3 minutes 49 seconds under *Windows* (only 2.7 times slower). The *Windows* version was also handicapped by consistently reporting an error stating that it could not find a particular file in the root directory of my hard disk. This was unsurprising as the file did not exist. I cannot explain such an action; very strange.

The disparity in the scan times so intrigued me that, for comparison purposes, I scanned the same disk with two other well known scanners. I also executed the DOS version of *Norton Anti-Virus* from a DOS box within *Windows*.

The following measurements (see Figure 1.) were obtained while scanning a 40 Mbyte hard disk containing 1545 files spread across 34 Mbytes of disk space.

Product	Integrity Check	Disk Scan	Total
Norton v2.0, DOS	9s	1m 24s	1m 33s
Norton v2.0, Windows	5m 06s	3m 49s	8m 55s
Norton v2.0, DOS box	17s	3m 05s	3m 22s
FindVirus (S&S) v3.5	10s	37s	47s
Sweep (Sophos) v2.35	-	1m 04s	1m 04s

Figure 1. Comparative execution times

This places *Norton Anti-Virus* operating under DOS in the same league as many other virus scanner programs, if not exactly up with the fastest. However it leaves the *Windows* version of *Norton Anti-Virus* somewhat out on a limb. When the DOS version of *Norton Anti-Virus* is executed in a DOS box under *Windows*, then it executes twice as slowly as under DOS, but still very much quicker than the pure *Windows* version.

I don't know whether the pathetic scanning speed of the pure *Windows* version of *Norton Anti-Virus* is due to *Windows*, *Norton Anti-Virus* itself, or a combination of the two. Frankly I don't care; I have better things to do than wait for nearly 9 minutes for a scan of my hard disk to be completed.

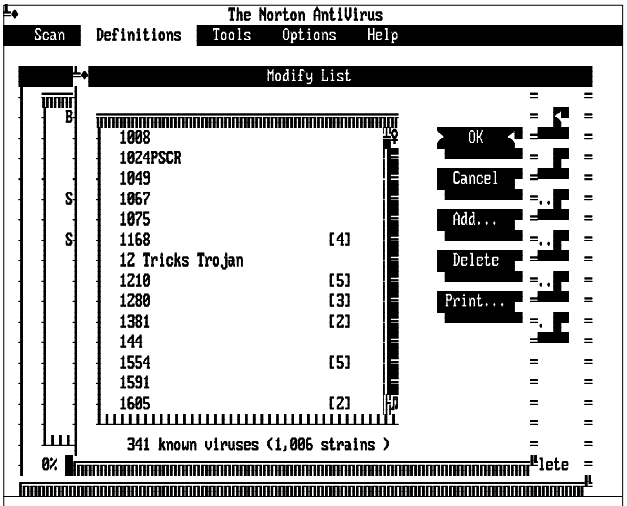
Last time I reviewed *Norton Anti-Virus*, I complained that the horizontal bar indicating progress during scanning had only reached about 40% of its full range when the software realised that it had completed execution and immediately zoomed up to 100%. It still does this.

Detection

I tested *Norton Anti-Virus*' detection capabilities against the viruses shown in the *Technical Details* section at the end of this review. Out of the 114 viruses (183 strains in total), *Norton Anti-Virus* detected all except six (Bebe, Jocker, Monxla, Rat, Terror and Turbo-488). None of these are new viruses, nor, I would venture to suggest, particularly difficult to detect. A failure rate of 6 out of 114 corresponds to a detection rate of 94.8%, which is somewhat better than the detection rate of 86.8% measured by *VB* for *Norton Anti-Virus* in the last comparative scanner review (*VB*, September 1991). It is worse than the detection rate measured in my original review of *Norton Anti-Virus* v1.0 in the January 1991 issue of *VB*, but my test sample of viruses then only comprised 49 viruses, with various strains providing 101 virus test samples. No matter how you view it, *Norton Anti-Virus* is not the best product on the market for accurate virus detection.

Scattered Files

The original version of *Norton Anti-Virus* had what it then called an 'Advanced scan' mode which created a hidden checksum file for every executable file, the first time that a



Known viruses and strains. *NAV* has a respectable detection rate and the product has been updated regularly since its release.

particular file was tested. Even though these small files were at most 77 bytes long, in reality each file occupied somewhere between 2 Kbytes and 8 Kbytes of disk space (depending on the version of DOS in use). This was heavily criticised (nay tittered at!) by myself and other reviewers as unnecessarily wasteful. The developers of *Norton Anti-Virus* have listened to such criticisms and *Norton Anti-Virus* now maintains a single file containing this information, which it refers to as inoculation data. This file is created automatically in the root directory the first time that a scan takes place on a disk and can be updated by the user as desired. It works rather well.

Virus Intercept

Virus Intercept is a memory-resident program, which detects copying and/or execution of virus infected files. During the boot process, the desired *Norton Anti-Virus* device driver loads virus definitions from file. This takes about 12 seconds, which extends the boot process somewhat, but is not too onerous. A user can choose one of three device drivers:

1) This detects viruses when an infected program is executed, and occupies just 1K of memory. It does not detect boot sector infections, and does not provide visible *Virus Intercept* alerts while under *Windows*.

2) This is exactly the same as 1), but does detect boot sector viruses, and can produce Intercept Alerts under *Windows*. It occupies 6K of memory.

3) This provides all of the above facilities, and also scans files during copying. This device driver can write-protect the partition table and boot sectors of a hard disk, and warn when anything attempts to alter these areas of the hard disk. It occupies 39K of memory.

By default the second option is selected.

I measured the overhead that device driver type 3) introduced when copying 578K of files from one hard disk subdirectory to another. Without *Norton Anti-Virus* present, this copy took 7.6 seconds. When the *Norton Anti-Virus* device driver was introduced, the copying time increased to 11.8 seconds, an increase of 55%.

It is inevitable that such monitoring for viruses introduces some detrimental effect on the speed at which files are copied, or at which programs can be executed. A 55% increase in file manipulation time is roughly the same as figures reported in *VB* for similar products (e.g. *PC Armour*, March 1992).

It should be noted that this overhead will vary widely from one type of file to another. For instance last time that *Norton Anti-Virus* was reviewed, I found that the increase in file copying time varied between 25% and 300%.

I've complained about it before, but still the *Norton Anti-Virus* documentation does not discuss the overhead imposed by *Virus Intercept*. Given that the intensive use of computer resources under *Windows* now makes the overhead readily visible, this is not good enough. Such an overhead is inevitable. Users should be given factual information about it, and allowed to make up their own mind about whether or not the extra delay is justified.

Conclusions

The installation program for *Norton Anti-Virus* is excellent. Indeed the overall presentation of the product, the documentation, and the operation of the *Virus Clinic* programs can hardly be faulted. In my previous review I was quoted as saying 'Suffice it to say that the manual needs completely rewriting before it can be much use to anyone except a beginner'. The documentation currently provided with the current version of *Norton Anti-Virus* is very good indeed.

Previously, I stated that '*Norton Anti-Virus* scans for files very quickly, and is now efficient at detecting viruses: a very worthwhile combination...'. *Norton Anti-Virus* is not the best performer around, but I've no real reason to change my conclusion as far as the DOS implementation is concerned. Although *Norton Anti-Virus* has some way to go to improve its detection rate to approach that of the market leaders, in mitigation, it has improved recently. Most developers of anti-virus products are finding the rate of arrival of new viruses somewhat daunting and the developers of *Norton Anti-Virus* will have to put in a lot of effort to keep up.

The scanning speed of the newly introduced *Windows* version of *Norton Anti-Virus* is lamentably slow. It must be improved before users with 'ordinary' computers can take it seriously.

In summary, I find *Norton Anti-Virus*'s program design and ease of use to be excellent. If you want a product that operates with a DOS version and a *Windows* version, in similar fashion for both environments, then *Norton Anti-Virus* comes as close to seamless movement between the two as it is possible to get. However, to make the scanning speed of the *Windows* version of *Norton Anti-Virus* even halfway acceptable, make sure you have a real screamer of a 486 machine. You'll need it.

Technical Details

Product: *Norton Anti-Virus*

Developer: *Symantec Corp*., 10201 Torre Ave., Cupertino, CA 95014-9854, USA, Tel: +1 (800) 441-7234, Fax: +1 (408) 255-3344, Bulletin Board: +1 (408) 973-9598.

UK Vendor: *Symantec (UK) Ltd*., MKA House, 36 King Street, Maidenhead, Berkshire SL6 1AT, UK, Tel: +44 (628) 776343, Fax: +44 (628) 776775.

Availability: IBM PC, XT, AT, PS/2 or 100 compatible, running DOS 3.0 or later. The *Windows* version requires v3.0 of *Windows*, and v3.1 of DOS. A hard disk with at least 800K of available space, and 384K of available RAM are both required.

Version Evaluated: 2.0R, updated with virus definitions up to 25th February 1992.

Serial Number: 0000610564

Price: Special offer to existing *Symantec* customers of £59+VAT. Usual price = £149+VAT. Annual subscription to make upgrades available = £100+VAT.

Hardware Used: Toshiba 3100SX laptop with a 16MHz 80386 processor, a 40 Mbyte hard disk, a 1.44 Mbyte floppy disk drive, and 5 Mbytes of RAM, running under version 5.0 of MS-DOS.

Virus Test Suite: This suite of 114 unique viruses (according to the virus naming convention employed by *VB*), spread across 183 individual virus samples, is the standard *VB* test set. It comprises two boot sector viruses (Brain and Italian), and 112 parasitic viruses. There is more than one example of many of the viruses, ranging up to 12 different variants in the case of the Tiny virus. The actual viruses used for testing are listed below. Where more than one variant of a virus is available, the number of examples of each virus is shown in brackets. For a complete explanation of each virus, and the nomenclature used, please refer to the list of PC viruses published regularly in *VB* :

1049, 1260, 12 TRICKS, 1600, 2144 (2), 405, 417, 492, 4K (2), 5120, 516, 600, 696, 707, 800, 8 TUNES, 905, 948, AIDS, AIDS II, Alabama, Ambulance, Amoeba (2), Amstrad (2), Anthrax (2), Anti- Pascal (5), Armagedon, Attention, Bebe, Blood, Burger (3), Cascade (2), Casper, Dark Avenger, Datacrime, Datacrime II (2), December 24th, Destructor, Diamond (2), Dir, Diskjeb, Dot Killer, Durban, Eddie 2, Fellowship, Fish 6 (2), Flash, Flip (2), Fu Manchu (2), Hymn (2), Icelandic (3), Internal, Itavir, Jerusalem (2), Jocker, Jo-Jo, July 13th, Kamikaze, Kemerovo, Kennedy, Keypress (2), Lehigh, Liberty (2), LoveChild, Lozinsky, MIX1 (2), MLTI, Monxla, Murphy (2), Nina, Number of the Beast (5), Oropax, Parity, Perfume, Piter, Polish 217, Pretoria, Prudents, Rat, Shake, Slow, Subliminal, Sunday (2), Suomi, Suriv 1.01, Suriv 2.01, SVC (2), Sverdlov (2), Svir, Sylvia, Taiwan (2), Terror, Tiny (12), Traceback (2), TUQ, Turbo 488, Typo, Vacsina (8), Vcomm (2), VFSI, Victor, Vienna (8), Violator, Virus-101 (2), Virus-90, Voronezh (2), VP, V-1, W13 (2), Whale, Yankee (7), Zero Bug.

END-NOTES & NEWS

The Cornell News Service announced on February 25th that two *Cornell University* students David S. Blumenthal, 19, and Mark Andrew Pilgrim, 19, were arrested and charged with computer tampering for allegedly distributing a computer virus via national computer archives. A preliminary hearing will be held on April 10th. The Macintosh virus MBDF-A was distributed in three games programs, Obnoxious Tetris, Terticycle and Ten Tile Puzzle which were uploaded to SUMEX-AIM at *Stanford University*, the *University of Texas* and to the *University of Michigan*. *Cornell University's Department of Public Safety* in conjunction with the *Tompkins County District Attorney's* office conducted the investigation. The *FBI* are also investigating breaches of federal law. *Cornell University's* previous famous computer prankster was, of course, Robert T. Morris whose worm program caused chaos on Internet in 1988.

John McAfee of *McAfee Associates* has resigned from the *National Computer Security Association's* anti-virus product developers' forum. It appears that at least two scanner 'certification' bodies will now develop in the United States. McAfee will support Patricia Hoffman's *Scanning Product Certification Scheme* while Dr. David Stang of *NCSA* presumably hopes that other vendors will not 'jump ship'.

The ***2nd International Virus Bulletin Conference***, Edinburgh, Scotland, September 2nd-3rd 1992. Details from Petra Duffield, *Virus Bulletin Conference*, UK. Tel 0235 531889.

IBM UK is conducting a **virus management course** (April 22nd) and a **virus 'hands-on' course** (April 23rd) in Manchester. Tel 081 864 5373.

Sophos is holding an **introductory 'hands-on' virus workshop** (May 26th) and an **advanced hands-on virus Workshop** (May 27th) in Oxford. Tel 0235 559933.

The *National Computer Security Association* is to hold the ***1st NCSA Virus Prevention Conference and Exhibition*** in Washington DC, USA, June 18-19th. Tel 717 258 1816.

Central Point Anti-Virus **version 1.2** is now available. The program 'detects both known and unknown stealth viruses in memory' - quite an achievement. Recommended Retail Price is £115. Updates at £19.50 plus P&P and VAT. Tel 0734 320314.

Computer Security Update is another **exciting new monthly newsletter** from Robert Schifreen (he of the notorious Prestel hack) and *Computer Weekly*. £295 annually, twelve pages an issue - a bit pricy but could be entertaining. Tel 081 652 3099.

Finally... The Michelangelo virus has played a minor role in the British election campaign. According to the *Daily Telegraph*, Prime Minister John Major's Private Parliamentary Secretary, Mr. Graham Bright had a disk trashed which contained a list of constituents and their voting intentions.

VIRUS BULLETIN

Subscription price for 1 year (12 issues) including first-class/airmail delivery:

UK £195, Europe £225, International £245 (US$395)

Editorial enquiries, subscription enquiries, orders and payments:

Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Abingdon, OX14 3YS, England

Tel (0235) 555139, International Tel (+44) 235 555139
Fax (0235) 559935, International Fax (+44) 235 559935

US subscriptions only:

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

Tel 203 431 8720, Fax 203 431 8165