January 1993 ISSN 0956-9979

VIRUS BULLETIN

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

CONTENTS

EDITORIAL

Imageline v. *McAfee*

The detection of a virus in an uninfected file is an all-too frequent occurrence with virus scanners. This is not always the manufacturer's fault, but the knotty problem of whether the anti-virus software vendor is in any way liable for any subsequent inconvenience has, until now, to be explored. This important question is about to be addressed in the United States, as *McAfee Associates* is being sued for $750,000 as a result of a false positive dispute.

The central issue in the case is not directly about a scanner detecting a false positive, but addresses the issue of what action the manufacturer is required to take when such a situation occurs.

The problem arose at the start of last year, when *McAfee Associates Pro-Scan* version 2.33 detected the 7808 virus in an executable sent out with some clip-art. *Imageline*, the producers of the clip-art, contacted *McAfee*, which updated its software, thus removing the false positive problem. At this point the dispute should have ended.

However, *Imageline* continued to receive complaints about its software being infected with a virus, although *McAfee Associates* assured *Imageline* that 'As far as *McAfee* can determine, it has distributed fewer than forty copies of *Pro-Scan* version 2.33.' By this time, *Imageline's* product had acquired a somewhat tarnished image, and so they implored *McAfee Associates* to inform all customers of the problem.

Imageline finally sought a court injunction which required *McAfee Associates* to stop distribution of that version of *Pro-Scan* and any third party products which used that version under licence. The injunction also ordered *McAfee* to inform all buyers of the product about the problem.

According to documents obtained by *Virus Bulletin*, *Imageline* is now suing for 'compensatory damages in the amount of $250,000 and punitive damages in the amount of $500,000'. In the complaint, brought in Civil Action Number 3:92CV710, *Imageline* claims that 'The mere accusation that computer software contains a virus threatens immediate destruction of the software's viability in the market. In the case of a start up company such as *Imageline*, such accusations create a substantial risk that the company could be forced out of business.'

Furthermore, the action alleges that 'As a direct, proximate and foreseeable result of the foregoing misrepresentation by *McAfee*, *Imageline* has been damaged. Such damages include, but are not limited to, the loss of sales opportunities and damage to *Imageline's* business reputation as a result of the false indications that *Imageline's* products are infected with viruses.'

Bill McKiernan, President of *McAfee Associates*, refused to comment on the case and simply stated that the suit is 'totally without merit' and that *McAfee Associates* 'will vigorously defend itself.'

The implications of this case are far-reaching. Arguably, false positives are becoming the overriding concern for both the anti-virus industry and the users. It is commercially damaging for a virus scanner to produce false positives - even more so than its missing a handful of viruses.

It is equally damaging to software which is erroneously identified as infected, as this can result in loss of confidence in the package. The question of how to act when such a situation occurs now needs to be addressed.

Every virus scanner is prone to false positives - it is something which occurs to all scanner manufacturers from time to time. Clearly a situation in which litigation can result from *any* false positive identification is ridiculous. In these circumstances, scanner manufacturers would have no choice but to shut up shop and return home.

If this case shows that a vendor has no responsibility for false positives produced by its product, a worrying precedent is set: if a company is sufficiently small, and its software is of limited circulation, an anti-virus vendor could simply ignore its plea for help. Put bluntly, if the problem is small enough, there is no financial incentive for the anti-virus manufacturer to set the record straight.

The results of this action may well affect those distributing shareware anti-virus software more than other vendors. It is far easier to inform users of a potential problem if they have purchased software directly than to trace users of an electronically distributed product, which could have been downloaded from one of any number of bulletin boards.

If it is shown that the onus is on the scanner manufacturer to deal with false positives, the problem of deliberately including scan strings within code raises its ugly head. It would then be possible to target a scanner, and force its vendors to alter search patterns. The even more complicated issue of scanners detecting virus patterns in other scanners could become a legal minefield. In such a world, only the brave or the foolish would produce a scanner.

Whichever way the case is decided there are stormy seas ahead for both the software industry and, more specifically, the anti-virus industry. *McAfee Associates* is certainly not the only scanner manufacturer who will be waiting for the results of the trial with bated breath.

NEWS

S&S Caught Out

Dr Solomon's *Anti-Virus Toolkit* has failed to detect a virus on some five hundred evaluation copies of a printer driver from Limerick-based software manufacturer *DCA*. The infected disks were sent to journalists throughout Western Europe and the Middle East.

A copy of the virus was subsequently sent to *S&S International* which identified it as a NoInt variant. Ironically, this new variant *was* detected by many other virus scanners on the market. It appears that the search string used by the *Toolkit* had been targeted and altered in the variant.

This incident again illustrates the danger of relying on one single package for virus detection - two or more unrelated scanners should always be used for critical machines. It also emphasises the shortcomings of using virus-specific detection. A sound anti-virus strategy should therefore always encompass integrity checking.

Placing a sticker on a disk which reads 'certified virus-free by *Acme Software*' is no guarantee of that disk's integrity. A more meaningful claim would simply state 'Scanned for viruses known to *Acme Software.*'

Before other vendors crow too much over *S&S's* misfortune, they should be reminded that such a mishap could have happened to any of them. Whose turn will it be next?

Chinese Whispers

De Telegraaf, the largest circulation paper in The Netherlands, recently ran the headline: 'Virus error in prescription almost fatal. Infected PC dangerous to human lives'.

The story described how a patient had nearly been given a lethal dose of morphine due to a computer virus which had infected pharmacy PCs used for drug dispensing. The virus known as Nines Complement is of interest because it transposes all printed digits between 0 and 9, such that a 1 becomes an 8, a 2 changes to a 7 and so on.

Such a dramatic story contains all the necessary ingredients to make front page news. Predictably, the original report rapidly became embellished beyond all recognition. On the early morning television there were reviews of the day's newspapers, and by mid-morning many people falsely believed that it was unsafe to take *any* prescribed medicine. The reports snowballed, and eventually messages on local radio stations were needed to reassure an understandably perplexed population.

The story originated at a press conference held by *Titia Electroniks*. This company acts as an agent for *Computer Security Engineers Ltd*, developer of the *PCVP* anti-virus package. *De Telegraaf* sent a financial editor, Klaus Steenhuis to the meeting. It was during this press conference that Steenhuis and assembled journalists were told, as an aside, how the Nines Complement virus had been found in a single pharmacy. From this small beginning grew *De Telegraaf's* front page news story.

The first report received by *Virus Bulletin* spoke of 'NineComp virus being endemic in pharmacies in the Hague, with hundreds of machines affected.' The number of machines that were *actually* infected in the original incident was, in fact, just two.

It is worthwhile looking to see who are the winners and losers in this story. The obvious loser is the Dutch public, which has lost still more faith in the computer and has had its technophobia reinforced. The winner was *De Telegraaf*, which gained a suitably lurid headline.

But what about the anti-virus industry? On the one hand, the report raised the public perception of the danger of computer viruses. On the other, such recurring sensationalism has further tarnished the industry's already less than shining reputation.

Exaggeration, misinterpretation and 'Chinese whispering' may well prove the downfall of a number of industry 'names' and organisations. In December, anti-virus supremo John McAfee was investigated in the *Wall Street Journal* while in Germany, *Der Spiegel* recently printed a blistering attack on well-known virus aficionados including Professor Klaus Brunnstein, *EICAR* and the *NCSA*.

True or false, such media antipathy damages the reputation of all those involved in the anti-virus field and undermines public confidence.

A Rose By Any Other Name

Until recently, *Virus Bulletin* provided the only recognised standard naming convention in the industry. However, at the *EICAR '92* conference held in Munich, *CARO* was strongly pushing its own standard naming convention for many of the viruses known to date. Although *CARO* names and *Virus Bulletin* names are reasonably compatible, there is still some disagreement between the two systems.

Greater standardisation of virus names will be of benefit to users worldwide. A great deal of confusion is caused by the current situation, where the same virus may have two or more different names. *CARO* intends to extend its work, and discussions are in progress about a proposed database of virus information, *CARObase*.

IBM PC VIRUSES (UPDATE)

Updates and amendments to the *Virus Bulletin Table of Known IBM PC Viruses* as of 24th December 1992. Each entry consists of the virus' name, its aliases (if any) and the virus type. This is followed by a short description (if available) and a 24-byte hexadecimal search pattern to detect the presence of the virus with a disk utility or preferably a dedicated scanner which contains a user-updatable pattern library.

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

Known Viruses

_288, Dismember - CN: A simple, encrypted virus, 288 bytes long.

```
_288            5D8D 5E0E B90F 01B0 ??30 0743 E2FB
```

_354 - CN: A 354 byte virus. Awaiting analysis, but might have been written by the author of the Loki virus.

```
_354            8B5D 09CD 21B4 3ECD 21B8 0143 32ED 8A4D 0BCD 21C3 1E07 FFE5
```

_377 - CN: A 377 byte virus. Awaiting analysis.

```
_377            FFE3 5225 00F0 3D00 F074 5F83 C31E 8BD3 B43D B002 CD21 8BD8
```

_547 - CR: A 547 byte virus. Awaiting analysis.

```
_547            9C3D 004B 7403 E95C 012E 8C16 2F02 2E89 2631 028C C88E D0B8
```

_889 - CER: A 889 byte virus. Awaiting analysis.

```
_889            3D00 4B74 03E9 2D01 FC2E C606 FD00 00B9 0001 1E07 B02E 8BFA
```

ARCV - EN: Several new viruses have appeared from ARCV recently, some of which are simple PS-MPC variant but others appear to be written from scratch. According to the 'president' of ARCV, the group has created over 40 new viruses, which can be divided into several groups. Joshua (965 bytes) and ARCV-7 (541 bytes) are related variants that do nothing particularly interesting. ARCV-7 will damage many of the files it attempts to infect.

```
ARCV-Joshua     BB?? ??B9 DA01 2E81 37?? ??83 C302 4975 F5
ARCV-7          BAFA FEBD ???? 2E81 7600 ???? 4545 4275 F5
```

AT-140 - CR: A 140 byte virus which does nothing but replicate. Like all other members of the AT family, it will only work on a 286 and above.

```
AT-140          8BE8 B18C 2BC1 3B44 0174 16B4 40CD F7B8 0042 33C9 CDF7 B440
```

Bit Addict - CR: A 477 byte virus. Awaiting analysis.

```
Bit addict      80FC 4B74 052E FF2E 1F00 2E80 3E23 0064 7226 B802 0033 DBB9
```

Cinderella-B - CR: A 390 byte mutation of the Cinderella virus. Detected with the Cinderella pattern.

Cinderella II - CR: This virus has been reported in the wild in Finland. It does not seem to be related to the Cinderella virus, but might have been written by the same author.

```
Cinderella II   80FC 4B74 0880 FC3D 7403 E924 0253 5106 5657 1E52 5055 8BEC
```

Cpw - CER: A 1459 byte virus, probably from Chile. Not fully analysed.

```
Cpw             80FC 4B74 2F3D 003D 742A 80FC 4374 25EB 1590 B42A CD21 81FA
```

Deicide II-Brotherhood - CN: Probably written by the same author as the other Deicide II viruses, and just as badly written as they are. This variant is 693 bytes long, and contains text messages indicating that it searches for some of the viruses it is related to.

```
Brotherhood     B440 BA00 01B9 9902 CD21 B457 B001 5A59 CD21 B43E CD21 8B1E
```

Girafe - CER: This ia a polymorphic, variable-length virus, which cannot be detected with a hex pattern. It includes the strings 'Amsterdam = COFFEESHOP!' '[MK / Trident]'. This seems to indicate that the virus is written by the same author as the MtE-Coffeshop virus, although it is encrypted in a different way. The virus activates on Thursdays, displaying a cannabis leaf, and the text 'legalize cannabis'. The most interesting feature of this virus is that instead of using MtE, it uses another polymorpic 'engine', which has been called TPE.

IPER - CR: A 1062 byte virus. Awaiting analysis.

```
IPER            5B80 3FE9 7403 E9BF 008B 4701 E83E FF81 C3C0 0089 07B8 0057
```

Kalah-499 - CR: Related to the Kalah virus, but somewhat longer. Detected with the Kalah pattern.

Kthulhu - CN: This 512 byte virus activates on May 20th, displaying the message 'Today is my birthday'.

```
Kthulhu         817D 1A48 EE77 E781 7D1A 5802 72E0 8BD7 83C2 1EB8 0043 CD21
```

Little Brother-361 - P: Yet another member of this family.

```
Little Br-361   9C06 1E50 5352 3D00 4B75 03E8 0B00 5A5B 581F 079D 2EFF 2E69
```

Loki - CER: A 1237 byte virus. Awaiting analysis. This virus will damage some files it infects.

```
Loki            33F6 33FF B900 01F3 A45E 560E 1FB9 0B05 F3A4 5FC3 0633 C08E
```

Malaise - CER: A 1355 byte virus. Awaiting analysis.

```
Malaise         9C3D 004B 7410 3D12 EF75 05B8 3412 9DCF 9D2E FF2E B601 2E8C
```

Mr. Virus - CN: A 508 byte virus which does not appear to do anything particularly interesting.

```
Mr. Virus       B440 8B5C 41B9 3E02 BA00 012B CA8B D62B D14A 8B4C 47CD 21B8
```

Ncu Li - ER: A 1688 byte virus. Awaiting analysis.

```
Ncu Li          A5A5 5F5E 071F 58C3 2EC6 0619 0100 509C 580D 0001 509D 58C3
```

PS-MPC - CN, EN, CEN: Several new PS-MPC-generated viruses have appeared recently. Any program able to detect the PS-MPC encryption method will detect them. However, as none of them are particularly interesting or have appeared in the wild, they will not be listed here.

Shadow - CEN: A 1200 byte virus. Awaiting analysis.

```
Shadow          5E83 EE0C 90BB 2F00 902E 8B54 2D90 2E8B 0033 C22E 8900 83C3
```

Storm, Tatou - CR: A 1153 byte virus. Awaiting analysis.

```
Storm           FA9C 3D00 4B74 143D FE4B 9075 07BD 3412 909D FBCF FB9D 2EFF
```

Timemark-1076 - ER: A new variant of this virus. Similar to those reported earlier, but with several minor changes - perhaps in order to avoid some virus scanners.

```
Timemark-1076   B8EE 4BCD 2172 03EB 6F90 0706 8CC3 4B8E DB8B 1E03 0083 EB44
```

Trivial 84 - CN: This virus overwirites the beginning of infected files, and makes no attempt to preserve their functionality, so it is extremely unlikely to spread. It can be disinfected, however, as it stores the overwritten code at the end of the file.

```
Trivial 84      2172 42BA 9E00 B802 3DCD 218B D8B4 3FB1 54B2 A051 CD21 722D
```

VCL-822 - CN: This variant calls itself 'Yankee Doodle 2', but that name should not be used. It is 822 bytes long, and detected in the same way as other VCL-generated viruses.

Vienna-598, -547 - CN: Two unremarkable Vienna variants detected with the W13 pattern.

Vienna-1054 - CN: A 1054 byte, encrypted variant.

```
Vienna-1054     81C7 F5FD B954 0390 8BF2 81C6 4901 33DB 8A3C 8A05 32C7 8805
```

Wilbur - CN: This 512 byte virus contains the texts 'Wilbur sez Hi!' and 'Origin: Berlin, Maryland 7Apr92'. It does not seem to do anything noteworthy.

```
Wilbur          7269 8BF5 81C6 C001 8BFE B920 008B 9EB8 01FC AD33 C3AB E2FA
```

Wizard - CR: A 268 byte virus. Awaiting analysis.

```
Wizard          80FC 4B74 052E FF2E F602 9C50 5351 5256 1E06 B801 43B9 2000
```

X-1 - EN: A 562 byte virus. Awaiting analysis.

```
X-1             0E1F 8C06 6C03 8C16 6E03 8926 7003 8CC8 0510 0033 DB4B 8BE3
```

Yankee-2885 - CER: This virus is derived from one of the TP variants (possibly TP 44), but has been changed considerably.

```
Yankee-2885     0376 2080 FC03 5053 5152 5657 1E06 9031 C050 0726 C536 4C00
```

INSIGHT

Scotland Yard's Virus Hunters

New Scotland Yard's Computer Crimes Unit (*CCU*) is not set in the somewhat glamorous surroundings of *New Scotland Yard*, but in a scaffolding-clad building immediately behind Holborn Police Station. It is from here that the *CCU* operates, monitoring all aspects of computer crime for the Metropolitan Police.

The aims of the *CCU* are set out in their seven point charter, reproduced below:

- ➤ The investigation of computer crime.
- ➤ To raise the level of awareness of the Police service as to the use of computers in crime.
- ➤ To train and advise officers how to investigate computer crimes.
- ➤ To raise the level of awareness within the information technology community as to how the Police service can assist them with computer crime related problems.
- ➤ To act as a liaison point for gathering of computer-related evidence.
- ➤ To provide a national collation point for liaison with telecommunication carriers.
- ➤ To provide a liaison point for reports of computer virus problems.

The unit consists of five officers who face a mammoth task: policing all incidents which fall into the category of crimes 'where a computer is the object of the offence.' This brief therefore neatly covers incidents involving hacking and computer viruses.

Trophies From The Hunt

Detective Constable Noel Bonczoszek has been with the unit for some years and has been integral to the unit's fight against computer crime. Simply walking around their office gives a feel for the unit's history. Pinned to the noticeboard is a signed extradition order for Popp, the man behind the AIDS diskette case. Below it sits a framed ten pound note bearing the legend 'Presented to Noel Bonczoszek from Chris Pierce' - the result of a bet over whether anyone would ever be brought to court for that case. The whole office is filled with mementoes like these - trophies from many years of hard work.

Seated looking out over London, with a steaming cup of strong coffee (part of the staple diet of the unit) Bonczoszek begins to explain some of the *CCU's* history and problems.

New Scotland Yard's Computer Crime Unit is located directly behind Holborn Police Station in the legal heartland of London.

One of the many hurdles the unit has to overcome is the reluctance of users to report computer crime. The *CCU* receives an average of three reports of virus outbreaks a week - a small fraction of the actual incidents which occur. Without receiving formal complaints from the public, however, the unit is powerless to act.

Many people still seem to treat computers as if they are somehow different from normal law. If a person forcibly entered a house without permission there would be no question as to whether or not the police should be informed, even if there was no damage done and no property stolen. When the same thing happens to a computer however, the victim frequently perceives the crime as far less serious.

Another part of the job is increasing the awareness of computers within the Metropolitan Police. 'After all,' points out DC Chris Pierce, 'computers are a tremendous aid to investigation.' Explaining to other units how to take advantage of this and the ways computers can be used as a tool to investigate crime, is a highly valued part of the job.

The *CCU* plays the role of a translator, providing specialist support to those who need it. 'One of our jobs is to act as an intermediary between the experts, the lawyers, and the victim. We have a very good overview of the situation, and know whom to contact for each specific problem we encounter. It's almost like being a system analyst of computer crime!' adds Pierce.

Each of the officers has their own area of specialist knowledge, but none would claim to be a 'computer wizard'. This is no drawback - a solid understanding backed up by acknowledged experts has helped make the unit a world leader in tackling computer crimes.

When asked if it was difficult to prove guilt to a jury of laymen in a complex technical case, Pierce replied 'No, not really. A jury is very good at distinguishing right from wrong. Our job is therefore simply to find an expert who is capable of explaining these complex issues in court.'

Unlawful Entry

Viruses are not by any means the unit's main concern. Many of the cases have involved disgruntled employees who attempt to take advantage of their privileged positions. 'In the days when everything was carried out on paper, five or six employees would need to work together to cover their tracks - now on a computer, one person can alter all the relevant information.' explains Bonczoszek.

Another typical scenario is the system which is operated by a single 'wizard'. To such an operator the system frequently acquires a life and character of its own, and he can become extremely possessive. 'Often we see an attitude of ''if I can't have it, you won't either'' ', adds Bonczoszek. Whenever a system is dependent on a single man, there is a built-in risk - nobody else can fully understand how things are structured. Bonczoszek strongly advises against relying on any one person: 'Somebody else apart from the system manager should be responsible for system security - don't put all your eggs in one basket.'

Most computer crime still goes on at a relatively simple level. 'At the moment computer hackers are using quite simple methods of hacking a system as many basic loop-holes have not been closed.' Pierce commented. 'The next wave of hackers will be much harder to deal with.' When many systems still have their factory preset passwords installed, it is small wonder that hackers have not resorted to using the more sophisticated weapons in their armoury.

'Ello, 'ello 'ello. From left to right: DC Chris Pierce, DS Steve Littler and DC Noel Bonczoszek.

Back To The Future...

What of the future? As virus code becomes more freely available it is an open question whether the law as it stands really protects the user. The *Computer Misuse Act* is largely untested, and only time will tell if charges placed now under the act will stand up in court. Pierce is confident that justice will be done - if the law proves to be weak, then new legislation will have to be put in place.

Pierce does not think there is a problem: 'Think of the *Computer Misuse Act* as the first *Road Traffic Act* - it had to be developed to protect the people as things changed. If the *Computer Misuse Act* needs to be developed, it will be.'

The relatively untested nature of the law is about to change. Last month an advert was run in a UK computer magazine, *Micro Mart*, offering for sale 'over 350 viruses, including boot sector, mutating viruses etc.' The advert went on to explain that these viruses should only be used for test purposes, and should not run under any circumstances.

On 10th December 1992, officers from the *CCU* working in conjunction with officers from the Warwickshire constabulary raided a house in connection with this advert. One man has been arrested for offences under Section 3 of the *Computer Misuse Act*.

Clearly Bonczoszek is reluctant to comment for fear of prejudicing the case. However, he did say that evidence had been seized and that the case would be referred to the *Crown Prosecution Service*. *Virus Bulletin* will cover the case in detail as soon as it comes to trial.

Success in these test cases is important - if this case proves that it is legal to trade malicious code, the door will be left open to anyone who wishes to do so, and Bonczoszek, Pierce and the rest of the team are present at a highly critical time. It is therefore vital that the unit gets full support from all those involved in this area in any way - especially from users and companies whose machines are hacked into or infected by a computer virus.

Because of the problems of proving an individual has written a virus and then deliberately spread it, some would doubt whether the unit can really help. When Bonczoszek is asked if the *CCU* can effectively do anything to fight the virus authors he smiles a wolf's smile: 'If we found out that the Dark Avenger was in Britain, of course we'd take action. And that's a promise.'

The mood within the unit is surprisingly optimistic - rather than being cowed by the prospect of an avalanche of viruses, they simply plug holes as they appear. 'We've got various things in the pipeline,' says Bonczoszek mysteriously, 'you can expect to see results in the future'

SCANNER UPDATE

Mark Hamilton

1993 Scanner Shoot-out

It is now six months since *Virus Bulletin* last pitted the ever-increasing number of virus scanners against the *VB* test-sets. This comparative review has proved to be the biggest ever, with 20 products tested.

The essential criteria which all products should meet are:

➤Their ability to detect viruses known to be in the wild.

➤Their ability to detect self-mutating strains.

➤Their concordance with each other.

Any well maintained scanner should score 100% against the 'In The Wild' test-set, as these are the viruses which it is likely to encounter. Another telling result is Mutation Engine detection. Even though the Mutation Engine has been known about since last March (see *VB*, April 1992, p.11), many scanners fail to detect it. In that edition *VB's* Technical Editor wrote: '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.' Far more than a couple of months have passed, and all scanners should get full marks.

The ability of the different packages to co-exist is measured in the concordance test. This test is of particular interest to anyone who wishes to use more than one scanner, as much time could be lost due to false alarms.

Two products submitted failed very early on in the testing process: the disks supplied with *Fifth Generation's Untouchable* product were unreadable, and *Leprechaun's Virus Buster* insisted on aborting with run time errors.

Allsafe Version 4.1

In The Wild	81.25%
Standard	94.51%
Enlarged	87.48%
Mutation Engine	0%

Xtree's Allsafe had file dates of June 1992, and it showed its age by performing poorly in all the virus detection tests. Particularly worrying is its failure to detect several viruses known to be at large. It also missed *all* the Mutation Engine infections and its false-positive identification of Anarkia in a text file provides an eye-opening insight to *Xtree's* detection strategy. A better result than last year, but still woefully inadequate.

Norton Antivirus Version 2.1

In The Wild	95.31%
Standard	98.63%
Enlarged	93.49%
Mutation Engine	94.14%

Symantec's Norton Antivirus proudly displays a sticker affixed to its packaging that proclaims 'Detects 100% of all viruses in the *NCSA* Library'. I have no information as to the precise contents of this library, but *Norton Antivirus* certainly does not detect all the viruses in the various test-sets used here. Its Mutation Engine detection algorithm needs tightening, as it detected only 1,446 of the 1,536 samples. Although the product did not fare too badly in any of the test-sets, its results were not outstanding. Most seriously, it missed viruses from the 'In The Wild' test-set.

Virex-PC Version 2.3

In The Wild	99.22%
Standard	98.90%
Enlarged	96.42%
Mutation Engine	99.93%

Virex-PC missed one virus, SBC, from the 'In The Wild' test set, but fared better in the Mutation Engine test-set, detecting all but one of the samples. However, *Virex* does have a problem with the concordance test: *AVScan* detected the signature for the 570 virus in this scanner, *Sweep* found signatures for Filedate 11-537, VCL-3 and Ryazan and *PC-Eye* reported an infection by USSR-1594.

Sweep Version 2.44

In The Wild	100%
Standard	100%
Enlarged	96.42%
Mutation Engine	100%

Another healthy result for *Sophos' Sweep*. Its recently overhauled scanning engine has helped make this one of the faster products tested.

Package	In The Wild 128	Standard 364	Enlarged 783	Mutation Engine 1,536	Overall Performance
Allsafe	104	344	685	0	78.82
AVScan	128	364	771	1536	99.92
Central Point AV & CPAV-SOS	125	353	705	Failed to complete	92.33
F-Prot	128	364	779	1536	99.97
HT-Scan	121	354	683	1446	94.72
Integrity Master	123	348	692	0	90.86
IBM AntiVirus	128	360	741	1536	99.62
McAfee Scan	128	360	751	1536	99.69
Norton Antivirus	122	359	732	1446	90.79
PC-Eye	126	361	732	0	93.34
Search & Destroy	125	356	735	1446	92.60
Sweep	128	364	755	1536	99.82
TBScan	126	358	715	1536	98.15
Toolkit (S&S)	128	362	776	1536	99.93
VI-Spy	128	363	763	115	94.85
Virex-PC	127	360	755	1535	94.09
Viruscure-Plus	103	296	505	0	75.74
VIS	127	364	782	137	94.37

Detection Results: The overall performance of each product is in the form of a percentage, where each of the test-sets is weighted according to their importance. The appropriate weightings are: In The Wild 80, Standard 10, Enlarged 5, Mutation Engine 5. The scores for the Mutation Engine detection are calculated on an all or nothing basis.

AVScan Version 0.98H

In The Wild	100%
Standard	100%
Enlarged	98.47%
Mutation Engine	100%

AVScan is a freeware scanner by *H+BEDV Datentechnik Gmbh*, a German software house. *AVScan's* scanning engine performed extremely well against all the test-sets, and was also one of the fastest scanners tested. *AVScan* is currently available on *CompuServe* where it can be downloaded from the Virus Help forum.

HT-Scan Version 1.19

In The Wild	94.53%
Standard	97.25%
Enlarged	87.23%
Mutation Engine	94.14%

HT-Scan is now in its 19th release and needs to be able to detect more common viruses, as it failed to find Father, PcVrsDs, Spanz and SBC from the 'In The Wild' test-set. *HT-Scan* uses an external module to detect Mutation Engine-encrypted viruses and this obviously needs further development - it missed 90 of the 1,536 infections.

Dr Solomon's Anti-Virus Toolkit Version 6.02

In The Wild	100%
Standard	99.45%
Enlarged	99.11%
Mutation Engine	100%

Problems were encountered with the *Windows* version of *Doctor Solomon's Anti-Virus Toolkit* when it came to detecting the Mutation Engine-encrypted samples. The first time I ran the test, the program reported that it had detected 1,474 files infected with viruses and that it had checked the same number of files. However, this test-set contains 1,536 infected files so I re-ran the test: again only 1,474 files checked. On the third run, this figure improved by one to 1,475. In each case it detected all the files as being infected. The final run provided me with the somewhat confusing results of 1,927 files checked with 1,925 infected files found (out of a possible 1,536 files)! This bug aside, both the *DOS* and *Windows Toolkit* performed very well

Central Point Anti-Virus and CPAVSOS Version 1.4

In The Wild	97.66%
Standard	96.98%
Enlarged	90.04%
Mutation Engine	Failed to complete

Two offerings from *Central Point Software* were entered: its commercial anti-virus product (*CPAV*) and a new, free, scanner-only version (*CPAVSOS*), which the company is distributing electronically. The principal difference between the two is that *CPAVSOS* has no cure capabilities. In terms of detection capabilities both versions fared the same, failing to detect the Father and Crazy Eddie viruses contained in the 'In The Wild' test set. *Central Point's* software suffers from a bug which meant that it failed to complete the Mutation Engine test, hanging the PC [*see p.21. Ed.*].

F-Prot Version 2.06b

In The Wild	100%
Standard	100%
Enlarged	99.49%
Mutation Engine	100%

These excellent scores speak for themselves.

Integrity Master Version 1.13d

In The Wild	96.09%
Standard	95.60%
Enlarged	88.38%
Mutation Engine	0%

The failure to detect any samples of the Mutation Engine, coupled with its poor performance in the 'In The Wild' test-set make this a disappointing result for this product.

IBM AntiVirus/Dos and IBM AntiVirus/2 Version 1.00

In The Wild	100%
Standard	98.90%
Enlarged	94.64%
Mutation Engine	100%

IBM AntiVirus is reviewed in this edition of *VB* (see p.18) so the reader is referred there for detailed information.

PC-Eye Version 2.1

In The Wild	98.44%
Standard	99.18%
Enlarged	93.49%
Mutation Engine	0%

PC-Eye performed tolerably well in the tests, even though it missed one Whale and one of the Tequila infections in the 'In The Wild' test set. Surprisingly, it is totally unable to detect any Mutation Engine-encrypted code; it is to be hoped that its author, *PC Enhancements*, develops and incorporates the necessary algorithms before viruses which use the Mutation Engine become commonplace.

McAfee Scan Version 99

In The Wild	100%
Standard	98.90%
Enlarged	95.91%
Mutation Engine	100%

McAfee Associates' Scan has consistently scored well in *VB* comparative reviews. This time is no different, although the results in the Standard test-set are a little disappointing.

Package	Hard Drive Scan "Turbo" Mode	Hard Drive Scan "Secure" Mode	Floppy Drive Scan "Turbo" Mode	Floppy Drive Scan "Secure" Mode
Allsafe	0:54	2:16	0:08	0:13
AVSearch	0:29	1:10	0:03	0:07
Central Point Anti-Virus	1:30	2:35	0:06	0:11
Central Point Anti-Virus-SOS	Not Applicable	2:35	Not Applicable	0:11
F-Prot	0:16	1:12	0:03	0:06
HT-Scan	0:52	1:59	0:08	0:41
Integrity Master	0:50	1:45	0:03	0:08
IBM AntiVirus	1:38 0:30	3:11 1:20	0:14	0:51
McAfee Scan	1:18	2:56	0:05	0:12
Norton AntiVirus	0:56	2:04	0:07	0:10
PC-Eye	0:20	0:59	0:04	0:44
Search & Destroy	0:36	1:29	0:08	0:11
Sweep	0:21	1:52	0:03	0:05
TBScan	0:18	1:06	0:03	0:50
Toolkit (S&S)	0:25	0:55	0:03	0:04
VI-Spy	0:39	4:00	0:03	0:38
Virex-PC	1:10	3:31	0:03	0:49
Viruscure-Plus	0:53	Not Applicable	0:09	Not Applicable
VIS	1:26	4:44	0:18	0:31

Speed tests: While detection is more important than speed it is interesting to note the wide variations in scanning speed. A high scanning speed does not necessarily mean poor detection - the most accurate scanner in the test, *F-Prot*, was one of the fastest. The two times shown for the *IBM* product are respectively for building its integrity database and scanning, and integrity checking only.

Search & Destroy Version 25.08

In The Wild	97.66%
Standard	97.80%
Enlarged	93.87%
Mutation Engine	94.14%

Search and Destroy is a new product which *Fifth Generation* launched just before the end of last year. Like *Untouchable*, *Search and Destroy* has been licensed from *BRM*. It failed to detect Father and Penza from the 'In The Wild' test-set and while it reported the Dir II infected file as corrupted by a virus, the virus name itself was displayed as garbage characters.

TBScan Version 5.02

In The Wild	98.44%
Standard	98.35%
Enlarged	91.32%
Mutation Engine	100%

ESaSS, the Dutch company which writes *TBScan*, has clearly spent a great deal of time improving its product's user interface. It now sports a smart menu-driven front-end program which makes it much easier to use. It missed two viruses from the 'In The Wild' set - SBC and Spanz - but otherwise does reasonably well and is one of the faster products tested.

Viruscure-Plus Version 2.41

In The Wild	80.47%
Standard	81.32%
Enlarged	64.50%
Mutation Engine	0%

IMSI's Viruscure-Plus includes a customised version of *McAfee Associates Pro-Scan* and this has the unenviable position of being the worst performer of all those tested. It missed too high a proportion of those viruses known to be at large - these include Father, Spanz, Vienna 2B, Warrier, Old Yankee 2, Penza, Spanish Telecom 1 and Spanish Telecom 2. It only found 81% of the infections in the 'Standard' test set, 64% of those in the 'Enlarged' test set and none of the Mutation Engine-encrypted samples. The version tested was unable to read any of the boot sector-infected disks - the only product to fail this test. These problems aside, *AVScan* detected the signature for the Slow virus in this scanner's executable file.

VI-Spy Version 10

In The Wild	100%
Standard	99.73%
Enlarged	97.45%
Mutation Engine	7.49%

Two things mar the performance of this product from *RG Software*. First, it was only able to detect only 115 of the 1,536 Mutation Engine-encrypted files and, secondly, *AVScan* detected the signature for Aircop within one of its executable files. In spite of this, *VI-Spy* continues to be a strong American contender.

VIS Anti-Virus Utilities Version 4.1

In The Wild	99.22%
Standard	100%
Enlarged	99.87%
Mutation Engine	8.92%

A disappointing result in the 'In The Wild' test-set and Mutation Engine test-set for this usually faultless scanner. *Total Control* has since informed *VB* that these problems are due to bugs in the software, which has just undergone a major upgrade, and that the version sent was part of an extended Beta test. The fact that the new version has been written in a high-level language and now features a *Windows*-like, DOS character-mode interface (a true *Windows* version is also supplied) has greatly impacted on its scanning speed: it is now the second slowest of all the scanners tested. *PC-Eye* reported that one of the *VIS* executable files was infected with the Not1491 virus.

Observations

Every product in this review should score 100% when tested against the 'In The Wild' test-set. It is also reasonable to expect a good score against the standard test-set, as all these viruses have been known for at least a year.

Mutation Engine detection is equally important, and is very much a case of all or nothing. If one sample is missed on an infected machine, the virus will simply continue its spread unabated. It is therefore unacceptable that some vendors, after many months of access to code, are still not achieving reliable MtE detection.

For many users, a scanner is the only line of defence against virus attack. If *your* scanner has performed badly, it is time to consider seriously just how well your PCs are protected.

The Test Sets

1. In The Wild

Where appropriate one genuine COM and one EXE file infection of: 1575, 2100, 4K, 777, AntiCAD, Captain Trips, Cascade 1701, Cascade 1704, Dark Avenger, Dark Avenger, Dir II, Eddie 2, Father, Flip (20 COM and 20 EXE), Hallochen, Jerusalem, Keypress, Maltese Amoeba, Mystic, Nomenklatura, Nothing, PcVrsDs, Penza, SBC, Slow, Spanish Telecom 1 (5 COM), Spanish Telecom 2 (4 COM), Spanz, Syslock, Tequila (5 EXE), Vacsina, Vienna 2A, Vienna 2B, Virdem, W13-A, W13-B, Warrier, Warrior, Whale (11 COM), Old Yankee 1 and Old Yankee 2.

The following genuine boot sector infections: Aircop, Brain, Disk Killer, Form, Italian Generic A, Joshi, Korea A, Michelangelo, New Zealand 2, NoInt, Spanish Telecom, Tequila.

2. Mutation Engine

This test-set consists of 1,536 genuine infections of the Groove virus which uses Mutation Engine encryption.

3. For details of the other test-sets used please refer to:

[1] Standard Test-set: *Virus Bulletin*, May 1992 (p.23).

[2] Enlarged Test-set: This unofficial test-set comprises 783 unique infections.

Technical Details:

All speed tests were conducted on an *Apricot Qi-486/25*. The Hard drive speed tests were the time taken to scan a 30Mb partition containing 1,645 files (29,758,648 bytes) of which 421 (16,153,402) were executable. The floppy disk used was a 720 Kbytes disk containing 7 files (675,454) of which 3 files (25,805) were executable.

VIRUS ANALYSIS 1

Tim Twaits

The CMOS1 Virus

It is rare that a virus introduces a completely new idea - most are simply adaptations of existing viruses with small modifications or additions. The author of the CMOS1 virus, however, seems to have managed to find a new approach. To the best of my knowledge it is the first virus which modifies the non-volatile system configuration data in the CMOS RAM in anything other than a destructive way: hence the name CMOS1.

In The Wild Origins

It was unusual to receive this virus from a user whose PC had been infected rather than from one of the many virus researchers and collectors. As such, it provides an insight into how a new virus is first detected and countered. The first suspicion of something amiss arose because of an error condition detected by the *Windows 3.1* 32-bit disk driver. It would have been easy to ignore the message, since *Windows* still ran successfully without using the 32-bit driver. Luckily somebody decided to investigate.

The first step taken was to attempt to scan the machine for known viruses. However, after performing a clean boot from a system diskette prior to running the virus scan, the hard drive could not be accessed. Armed with this knowledge of the symptoms, the investigator identified another infected machine. Both machines were immediately isolated and all associated diskettes quarantined.

At this point I received a copy of the virus. As soon as a recognition pattern had been extracted, a complete scan of all machines and disks was undertaken. In this case the virus had been contained and no new infections were discovered. The source of the infection was later traced to a golf game which had recently arrived from Taiwan. This game had also been sent to an office in South Africa, so the virus may well have spread further afield.

Operation

CMOS1 is primarily a master boot sector virus. When the computer is booted from an infected disk the virus gains control. It creates a 'hole' in memory by decrementing a data value in the ROM BIOS data area which contains the useable memory size. This has the direct effect of reducing the available DOS memory by 1K. The virus then installs its own Interrupt 13h handler, which intercepts all calls to the BIOS disk services, before allowing the boot sequence to continue normally.

CMOS Modifications

The CMOS battery backed RAM in an IBM compatible PC contains the non-volatile system configuration information. The CMOS1 virus modifies this information to indicate that there is no A: drive attached to the computer. This appears to be an attempt to force the PC to boot from the C: drive in all circumstances, thus ensuring that the virus is always resident in memory. This in itself provides cause for concern, but more worryingly, it seems as though the author then intended the machine to reboot from the correct drive.

If this strategy had been successful it would be impossible to achieve a clean boot and the virus would be very difficult to detect. Fortunately, the author has made a number of false assumptions which mean that the virus will never function as described on a truly IBM compatible machine. However, be warned - presumably it worked (at least to some extent) on the virus author's machine.

This virus fails in its attempt to prevent a clean boot, but it must be asked whether such a feat is feasible. The answer to this could have a large impact on the viability of current virus detection procedures.

Because of the variations between PC BIOSes, it would appear that the boot sequence varies between machines. On the machines on which I tested this virus, the Power On Self Test routine detected the presence of a floppy disk drive regardless of the CMOS contents. This function appears to be reasonably standard, so this technique is highly unlikely to be the basis of a successful virus.

Infection

The virus always infects drive 80h (normally drive C) immediately after booting from an infected diskette. Further diskettes are infected when their contents are read. Thus simply inserting a diskette and typing DIR A: will cause the diskette to become infected. When infecting a disk, the virus needs to keep a copy of the original boot sector so that the boot sequence can be completed successfully after the virus code is executed.

On a hard disk the original MBS is stored in sector 17, cylinder 0, head 0. On a diskette an extra track (number 40 or 80, depending on the disk size) is formatted at the end of the normal data area. Creating this extra track has the advantage that the storage capacity of the diskette is not affected. However, not all systems can access this extra track successfully, and this will cause some machines to hang when booting from an infected diskette.

Stealth

The virus intercepts all requests to read the master boot sector and returns the contents of the original sector to the caller. This effectively hides the virus from scanning software unless a clean boot is achieved. It also provides the mechanism by which the virus invokes the original boot code at initialisation. The virus issues an INT 19h call to restart the system once the intercept handler is installed. The system then starts normally since the bootstrap code will now load the original boot sector.

All requests to write to the master boot sector are also intercepted, allowing the write operation to complete but then immediately re-infecting the disk. The result is that one can run utilities which modify the boot sector, such as FDISK, without displacing the virus.

The virus contains another feature, which could perhaps be described as stealth. As well as overwriting the code in the master boot sector, the virus also overwrites the partition table with invalid data. Thus when booting from a clean system diskette the hard drive cannot be accessed directly. Although one cannot scan the drive to detect the virus, the absence of logical drive C betrays its presence.

Increased Contagion And Trigger

In an attempt to make itself more contagious the virus will infect some EXE files written to drive A. The infection routine is primitive, as the file is simply overwritten by the virus. The program infects drive 80h immediately upon execution. This type of infection occurs whenever data starting with 4Dh (the EXE header identifier) is written to sector 3 on any cylinder of the diskette. This not only produces infected EXE files but will also corrupt any files which contain a sector starting with 4Dh.

While the creation of infected program files will undoubtedly help the virus to spread, it also significantly reduces the chance that the virus will survive in the wild. Since the infected programs are overwritten with the virus code they no longer retain their original function, providing an immediate signal that something has gone awry. While I do not think that it is beyond the (limited) technical ability of the virus author to devise a more sophisticated strategy, the code size has been restricted to less than 512 bytes, and there is simply no room for a routine which would make this virus truly multi-partite.

A proportion of EXE files written to fixed drives will be similarly modified, although in this case the modified program has a more disastrous effect. It will overwrite the first track of the first fixed drive, effectively making all data inaccessible. The data on any diskettes is also overwritten. These files are only produced when writing the EXE header to sector 3 on any cylinder in the range 512-767. The disk must contain a significant amount of data before this occurs.

Removal

After performing a clean boot, one can detect the presence of the virus both in the boot sector and in any files by using a simple search pattern. It is important to check data files as well as executables, since they may have been corrupted. If the machine is one which can be prevented from booting from the A drive, it is possible to erase the CMOS contents by removing its battery.

The virus can be removed from the Master Boot Sector on hard disks by copying the original contents which were stored by the virus (sector 17, cylinder 0, head 0) back to the boot sector (sector 1, cylinder 0, head 0) using a disk editor such as *The Norton Utilities*. Alternatively, the Master Boot Sector can be rewritten by using the FDISK /MBR command or by performing a low-level format. Be warned that because the virus corrupts the partition data stored within the Master Boot Sector, using the FDISK /MBR command will not recover the data stored on the drive; it will simply overwrite the virus code.

CMOS1

Aliases:	None known.
Type:	Resident semi multi-partite.
Infection:	Master boot sector and EXE files.
Recognition:	
System	Hard drive not accessible after clean boot. *Windows 3.1* 32 bit disk driver will not load. Location 28h in Master Boot Sector is 7Ch.
Hex Pattern	`B0FF E621 BA80 00B9 0100 B811 039C 9A?? ???? ??FE C680 E607`
Intercepts:	Interrupt 13h for stealth (boot sector only) and infection.
Trigger:	Creates Trojanised EXE files when writing to certain areas of a disk. The programs destroy disks.
Removal:	See text.

VIRUS ANALYSIS 2

Jim Bates

DOSHUNTER - Search And Destroy

People often ask me if I get bored constantly disassembling viruses and I must admit that there are times when I find it difficult to maintain the spark of interest. It is usually the simplest, most primitive viruses that provoke this ennui but the latest virus to arrive on my desk, in spite of being one of the simplest that I have recently examined, provided a refreshing change from the malicious intricacies of Starship and Commander Bomber.

As reported in the *End Notes and News* of last month's *Virus Bulletin*, various alarms of a vicious new virus have been received from the Netherlands recently and it proved difficult to determine precisely what the problems were. Finally, a specimen copy was sent to me for disassembly.

The virus is named internally as DOSHUNTER and in spite of the alarmist nature of the reports, analysis shows it to be nothing more than an extremely primitive overwriting virus. However, the code does contain a destructive trigger routine that executes on a system date of June 26th (any year), overwriting the data held on drive C.

Installation

The virus begins by checking whether the system date is 26th June. If it is, processing is immediately transferred to the trigger routine. On other dates processing continues by moving the host file to a position beyond the end of the file in memory and repairing it.

Next, an 'Are you there?' call is made by inserting a value of C600h into the AX register and issuing a DOS INT 21h function call. If the virus is resident in memory, this call returns with 07B7h in AX.

It should be noted that this call may cause problems with some older *Novell NetWare* systems which use a similar subfunction request to set a compatibility mode.

If the 'Are you there?' call is answered, processing passes to the host file. However if the virus is not already memory-resident, the existing INT 21h vector is collected and stored within the virus data area. A new memory block at the top of memory is created by dividing the existing block into two and the virus code is moved into it. Finally, the virus' own INT 21h handler is hooked into the system and then the host file is repaired in memory and executed.

Operation

While resident, the virus intercepts only the DOS Load and Execute calls (function 4B00h) issued to the system. As with the rest of the virus code, the routine is primitive and makes only the most rudimentary checks on potential targets for infection. The first check ensures that the first letter of the target filename extension is 'C' - this excludes EXE and overlay files but could still cause problems on a system where segmented executable code is used from files which match this criterion (*.COD or *.CEX for example).

The virus checks whether a file is already infected by opening the file and reading the first 483 bytes into memory. Then the word at offset 6 is tested for a value of 061Ah. If the target file is found to be infected, the file is closed, the attributes and date/time stamp are repaired and the original system request is allowed to continue unmolested. If the file is not infected, a check is made to determine that the size of the target file is above 483 bytes (which is also the overall length of the virus code).

"When the system date is 26th June, the trigger routine is invoked. This attempts to overwrite the first 128 sectors of drive C"

Once the suitability of the target file has been verified, the virus copies the first 483 bytes of the program file and appends them to the end of the file. Then the complete virus code is written to the beginning of the file and the file attributes and date/time stamp are restored to their original value, thereby concluding the infection process. Thus infected files will be 483 bytes longer than they were and the virus code will be at the beginning of the file.

There are some errors within the virus which will cause system malfunction. The main one involves the way that the virus attempts to avoid the DOS error reporting functions. The DOS error handler is disconnected during the infection routine but is not reconnected properly afterwards. Thus the next error condition encountered is likely to send the processor on a voyage to nowhere. This is probably how the virus came to be reported in such a garbled fashion.

Terminate With Extreme Prejudice

When a system date of 26th June is detected, the trigger routine is invoked. This attempts to overwrite the first 128 sectors of drive C with garbage. If successful, this will

destroy the vital system and file management areas of the disk and result in the loss of data. Recovery may be possible in some instances but will be a long and expensive process. After the overwriting routine has completed, the virus displays the message:

```
DOSHUNTER I ACTIVE. (C) ACORN.
```

The significance of the June 26th date and the '(C) ACORN' message are not immediately apparent.

Removal

As with all parasitic viruses, the best method of removal is to reboot the machine from a clean system floppy and then replace all infected files with clean originals. It is possible to repair files by replacing the virus code with the last 483 bytes of the file and truncating the file length by 483 but this is really a job for an expert and must be undertaken with care in a clean machine environment. Note that under certain circumstances, COMMAND.COM will become infected and this will invariably result in unpredictable system behaviour.

DOSHUNTER

Aliases:	None known.
Type:	Parasitic, overwriting virus.
Infection:	*.C?? files greater than 483 bytes in length.
Recognition:	
Files	Word value of 061Ah at offset 6 in the file.
System	0C00h value in AX and INT 21h returns 07B7h in AX if virus is resident.
Hex Pattern	`3D00 4B74 0E3D 00C6 7405 2EFF 2EDF 02B8 B707 CF06 531E 52B9`
Intercepts:	INT 21h, function 4B00h for infection and INT 24h for internal error handling.
Trigger:	Overwrites first 128 sectors of drive C: with garbage, uses INT 26h Absolute Disk Write.
Removal:	Specific and generic disinfection is possible. Under clean system conditions, identify and replace infected files.

VIRUS ANALYSIS 3

Penza - Variations On A Familiar Theme

Reports have been received from users in the north of England of the Penza virus at large. This sample is another relatively primitive virus. It is 700 bytes long, and the code is stored in a non-encrypted form. Complete disassembly took only a few minutes and it was immediately apparent that the writer has copied certain techniques from other viruses, notably the interrupt stripping (sometimes called tunnelling) routines introduced some time ago by the Eastern European virus writers.

The Penza virus infects any executable files (regardless of the file extension) which are between 513 and 65535 (inclusive) bytes in length. The infection technique used when the target file is segmented (the most common example of this is a .EXE file) mirrors that used in some other early viruses: the file is made into a binary image type by overwriting part of the header and then appending a segment relocation routine. The overall change in length caused by this modification is 700 bytes.

Installation

When invoked, the virus code sends an 'Are you there?' call consisting of placing a value of FF00h in AX and issuing an INT 21h function request. If the virus is resident this returns with FF00h in the CX register. If the virus is already memory-resident, the host file memory image is repaired and control is passed to it. If this is not the case, processing passes into the installation routine within the virus code.

The virus then creates a new memory control block at the top of conventional memory and copies the virus code into it. The existing address of the DOS INT 21h service routine is collected and stored.

Effective Stripping

One of the more interesting parts of the virus is the way it locates the original DOS INT 21h vector. This technique, known as interrupt stripping or tunnelling allows direct access to the DOS INT 21h call. This is done by taking advantage of the single-stepping interrupt, INT 01h, which causes an INT 01h call to be made after every instruction. The virus simply installs a temporary INT 01h handler and issues an INT 21h request.

The resulting code is single stepped through, with control returning to the virus' INT 01h handler between each instruction. The virus continues this single stepping until it

detects that it is now executing the original DOS INT 21h handler. The memory address of this handler is stored, and from this point on any DOS INT 21h calls are made directly to the DOS INT 21h handler.

Once an acceptable address has been found, the INT 01 routine disables itself by resetting the single step trap flag. No attempt is made to repair the INT 01 vector address. As this is rarely used by ordinary software, it is unlikely to cause noticeable problems except when attempting to run software debuggers etc. Once the installation routine is completed, processing is returned to the host file.

Infection

The virus intercepts requests for function 4B00h of the DOS services interrupt INT 21h and immediately installs a dummy error handler into the INT 24h vector position. This ensures that DOS will not report any spurious error messages to the screen.

Any restrictive attributes of the target file are then removed and the file is opened. The date and time stamp of the file is collected and stored and the file length is checked. If the length is between 513 and 64735 (inclusive) it is considered suitable for infection, otherwise the interrupt request is allowed to continue. The last two bytes of the opened file are then examined to see whether they are C7h and 07h respectively. If so, the file is considered to be already infected and processing continues into DOS.

If the virus deems the file suitable for infection some attempt is made to determine the file type. If the file begins with 'MZ' (indicating an EXE file), the virus inserts a jump instruction to the byte beyond the end of the program (thus making it into a COM type file). The virus code is then appended to the file before the relevant repairs are completed to the target file and processing is allowed to continue. Infected files show a size increase of 700 bytes.

Thus EXE files will first execute the virus code and then jump to a segment relocation routine which will undertake the same relocation that DOS does when executing EXE type files. COM files execute the virus code and then jump back to their own initial instruction.

Disinfection

While it is possible to disinfect files by replacing the modified byte and truncating the file, this is quite involved and might well be different if there are other similar strains of this virus around. Disinfection is really a job which should be left to the experts, and then only as a last resort. It is usually far safer to replace the infected file with an uninfected backup.

Payload

Although this virus does contain a trigger routine, the conditions for its execution are quite rare, so few people are likely to witness it under ordinary conditions. After the infection routine, the virus tests the last five bits of the system clock and if they are all zero, the trigger routine will be invoked. This condition happens once every 32 clock ticks of the clock, thus there is only a 1 in 32 chance of this happening during infection. When it does happen, the following message is displayed:

```
Welcome to Penza!
```

This is followed by a beep from the speaker. After this, processing continues normally by loading and executing the target file.

PENZA

Aliases:	None known.
Type:	Parasitic file infector (including COMMAND.COM under certain circum stances).
Infection:	Any executable files between 513 and 64735 bytes long.
Recognition:	
Files	07B7h as the last word in the file.
System	FF00h in AX returns the value FF00h in CX after INT 21h.
Hex Pattern	

```
CF32 C0CF 9C50 3500 4B75 03E8
0E00 583D 00FF 7502 8BC8 9DEA
```

Intercepts:

INT 21h for infection, 'Are you there?' call and detection of trigger condition.

INT 24h for internal error handling.

INT 01h to enable stripping of INT 21h.

Trigger:	Displays message 'Welcome to Penza!'
Removal:	Specific and generic disinfection is possible. Under clean system conditions, identify and replace infected files.

PRODUCT REVIEW 1

Mark Hamilton

IBM AntiVirus

When *IBM* announced the release of its new anti-virus package at a breathtaking price of $29.95 minor tremors were sent throughout the industry. The software is the result of five years' research and development by *IBM Research* [*For an interview with one of the authors of this package, see VB, December 1992, p.6. Ed.*]. There are currently two versions available: *IBM AntiVirus/DOS* which contains both the DOS and *Microsoft Windows* versions of the product and *IBM AntiVirus/2* which has the *OS/2*-hosted version. Both versions are delivered on two 3.5-inch, double-density diskettes accompanied by a 38-page manual.

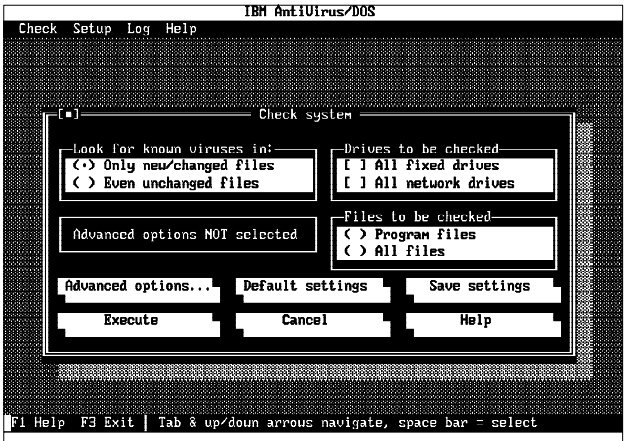
I have tested both versions of the product and they perform identically in terms of their virus detection capabilities. However, there are some differences in their functionality, and where this occurs I will draw the necessary distinctions.

Installation

IBM's previous anti-virus product, *VirScan*, consisted of a scanning engine, a signature file and disk-based documentation. *VirScan* was a command line-driven program which provided a large number of configurable options set by using switches on the command line. User-friendly it was not, but it got the job done. All this has changed - and changed radically - with *IBM AntiVirus.*

The installation process is simple and easy to follow. The installation program starts by checking its own integrity before checking memory for known viruses. Once this process is complete the user can then set the various configuration options.

You are given the choice of installing just the DOS version or the DOS and *Windows* versions (except for the *OS/2* version). Having made your choice, the installation program calculates the amount of disk space required, and displays this along with a list of all local fixed drives and their free space. This is a nice touch - with so much software being issued in compressed format, it is impossible to judge how much disk space it will require, and few users are aware of exactly how much space their hard drive has available. Another nice feature is that the programs are not too disk hungry - the DOS version requires approximately 720 kilobytes of disk space and the *Windows* version requires approximately twice this.



IBM AntiVirus attempts to combine the benefits of an integrity checker and a scanner in one easy to use package.

Having selected the drive, the installation program copies the relevant selected portions to the hard disk. You are then asked whether you wish to have your AUTOEXEC.BAT file updated. If you elect not to allow this, an example file is created in the product's home directory.

The next step consists of making an initial check of your files and constructing a database containing their integrity information. Before adding each file's characteristics to the database, it is scanned for viruses and then the relevant integrity information is extracted.

Automatic Detection

IBM AntiVirus has been designed as an 'install and forget' product - once installed you may never need to run any of its programs manually. The product is configured to be run automatically at boot time, and at the end of the installation process the frequency of the checks is set. This can range from 'Every Boot', 'Daily', 'Weekly', 'Monthly' to 'None'. The OS/2 version provides a further option to enable the PC to run the program at a particular time of day. *IBM AntiVirus* added 30 seconds to the boot-time of my machine to check the 421 files it considered executable.

All the versions of *IBM AntiVirus* run as menu-driven, mouse-aware full-screen applications but with a command line parameter that instructs the program to run without human intervention. This 'auto-pilot' mode is automatically disengaged if any virus-like activity is detected.

Boot Sector Oversight

If it can, *AntiVirus* always checks the Master Boot Sector and the active Partition Boot Sector and here I noted a weakness. The *Apricot Qi-486/25* used for this review has

both MS-DOS and *OS/2* installed, with the active Partition pointing to *IBM Boot Manager*. At boot-up time *Boot Manager* displays a menu which allows me to choose which operating system I want to use.

While testing to see if the product is capable of checking the DOS boot sector even though it is not marked as active, I discovered that I could make changes to this sector with impunity. *IBM* has since explained that the scanner does not use heuristic analysis on boot sectors, as no successful algorithm has been developed - this is still being worked on. However, it does successfully scan for known DOS boot sector viruses, regardless of the presence of *Boot Manager*.

Innovation

IBM AntiVirus is different from many of its competitors in that it combines an integrity checking method with a scanner. Whenever *AntiVirus/DOS* is asked to check a drive or set of files, it checks to see whether a database entry exists for each file. If one does, the program examines the integrity 'record' of the file against its previously stored entry. If they are identical, the next file is processed. If they do not - that is to say, the file has been modified in some way - it is scanned for viruses and the file is classified according to the results of the scan.

If any inconsistencies have been detected, the program displays its 'Results from check for viruses' dialogue box which contains three list boxes. If a file has been attacked by a virus and that virus can be positively identified and a cure exists within *IBM AntiVirus*, an entry appears under 'Verified as infected'. The file name is listed together with the virus and you can disinfect, erase or ignore all or any of these infections.

If a file has been attacked by a virus and it cannot be cured, then its details appear in a second list box entitled 'Probably infected'. Files can either be erased or ignored.

If a file has changed but does not contain a known virus, *IBM AntiVirus* will attempt to determine, by heuristic analysis, whether the change was as a result of virus infection or by some other means. The results of this examination appear in the 'Suspicious' list box. Again, you can either ignore or delete files listed here.

The integrity database only contains entries for files that are completely clean and have not appeared in any of these list boxes - there is therefore no chance of a virus accidentally slipping through!

IBM's 'install and forget' philosophy is quite acceptable and does not ignore the fact that you might want to perform one-off checks of diskettes. To cover this, the program includes menu options for checking diskettes and other drives. In this latter case, the configuration options are stored separately from those pertaining to the automatic tests. Therefore, for speed purposes, you could set up the automatic checking of just COM and EXE files at boot time and configure the manual checking for other file types. This could then be run overnight or during a lunch break. There are also facilities to check single files. The package is highly configurable - right down to the warning message which appears whenever it detects a problem.

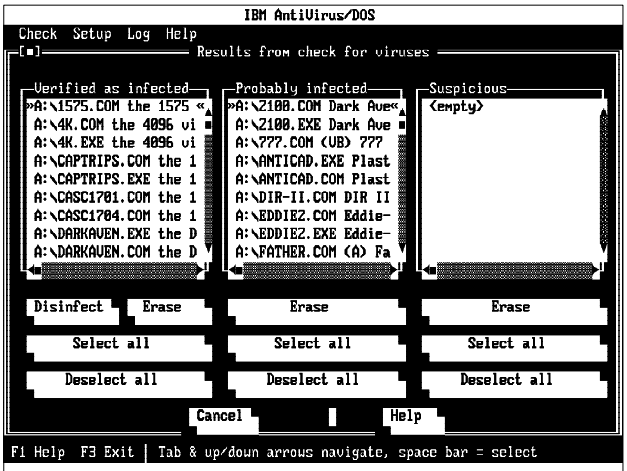
If problems are detected, the program suggests undertaking a full check of all available drives. This is a very wise precaution and is the default action.

Under *OS/2* and *Windows* Enhanced Mode all the checking can be performed in background. Under *OS/2* the load was significantly less than *Windows*, and the 30 seconds which the product added to the boot time of my system under DOS completely disappeared.

Scanner Accuracy

In tests, *IBM AntiVirus* detected all the viruses in the *Virus Bulletin* 'In The Wild' test set, missed four samples contained in the 'Standard' test set and detected 94.5% of infections in the unofficial 'Expanded' test set. In the 'Polymorphic' test-set it failed to detect any samples of the V2P6 virus which dropped its performance to 66%.

A new test set has been introduced this month - the 'MtE' test set. This test-set is made up of 1,536 genuine infections of the Groove virus, which uses Mutation Engine encryption. This product successfully detected all 1,536 infections, achieving an impressive 100%.



Files fall into one of four categories: Infected, Probably Infected, Suspicious and Clean. This may come as a shock for those accustomed to the usual True/False scanner output.

In addition to these good test results it successfully flagged as 'Suspicious' those files I intentionally changed - regardless of the type of change or whether the change was in the middle or at either end of the file. I also deleted its database and was gratified to discover that it assumed no database existed and therefore built one from scratch - by scanning the files for viruses first and refusing to include any that were in any way suspicious or, indeed, infected. All in all, its detection capabilities are highly creditable.

Both the *OS/2* and DOS versions provide a memory-resident detector which, *IBM* claims, can disinfect viruses in memory and warn if an infected program is run. If enabled under DOS 5, this occupies 640 bytes of conventional memory and the rest of the code is relocated into EMS. The *OS/2* DOS shield is capable of protecting all Virtual DOS Machines.

It is worth pointing out that the integrity shield can only detect viruses that are at large - it does not detect the vast majority of viruses which, so far, have not been circulated outside the virus writing and anti-virus communities. This is a double-edged sword because the user has no control over which viruses the shield is capable of detecting - a virus which is believed not to be in circulation one day may well appear 'in the wild' the next.

The rationale behind *IBM's* thinking is that the main program can disinfect any viruses thrown up by the DOS session shield. I would prefer it if the session shield could detect all viruses regardless of whether or not they are known to be 'in the wild' - this is a far more secure strategy.

All versions have comprehensive context-sensitive on-line help. This includes not only generalised help topics, but a tutorial about viruses, and a large number of virus descriptions - especially those in the wild.

Conclusions

This is an effective product that has been well thought-out; it is also a product that is in continuous development and *IBM* promises to include greater degrees of functionality and security with each subsequent release.

Having read this, you might decide you want to buy a copy of *AntiVirus/DOS* or *AntiVirus/2*, or indeed both, particularly since they cost $29.95 each!

However, *IBM* has the policy is that it is up to each country to decide if it wishes to stock an *IBM* product, and to date the product is only available in the US and Holland. It is to be hoped that *AntiVirus* becomes widely available, as at the price it provides unbeatable value for money, and outperforms some products which cost many times as much.

IBM AntiVirus

Scanning Speed

Hard Disk:	
Integrity Checking Only (Normal Operation) (538.4 Kbytes/sec)	30 secs
Scanning and building database (170.0 Kbytes/sec)	1 min 38 secs
Floppy Disk:	
Scanning and building database	14 secs

Scanner Accuracy

VB Standard Test-set[1]	360/364	98.90%
Expanded Test-set[2]	741/784	94.51%
'In The Wild' Test-set[3]	116/116	100.00%
'Polymorphic' Test-set[4]	100/150	66.67%
'MtE' Test-set[5]	1536/1536	100.00%

Technical Details

Product: *IBM AntiVirus/DOS* and *IBM AntiVirus/2*

Version: 1.00

Author: IBM AntiVirus Services, 1 East Kirkwood Boulevard, Roanoke, TX 76299-0015, USA

Telephone: +1 (800) 551 3579 for a single copy.
+1 (800) 742 2493 for site licenses and a full range of services.
+31 30 383816 (companies in the Netherlands).
+45 93 45 45 ext 3341 (companies in Denmark).

Fax: +1 (214) 235 9586

Price: $29.95 each.

Test Hardware: All tests were conducted on an *Apricot Qi486* running at 25Mhz and equipped with 16MB RAM and 330MB hard drive. *IBM AntiVirus* was tested against the hard drive of this machine, containing 1,645 files (29,758,648 bytes) of which 421 were executable (16,153,402 bytes) and the average file size was 38,370 bytes. The floppy disk test was done on a disk containing 7 files of which 3 (25,508 bytes) were executable.

For details of the test-sets used, please refer to:

[1] Standard Test-set: *Virus Bulletin* - May 1992 (p.23).

[2] This unofficial test-set comprises 784 unique infections.

[3] In The Wild test-set: *Virus Bulletin* - January 1993 (p.12).

[4] Polymorphic test-set: *Virus Bulletin* - June 1992 (p.16).

[5] MtE test-set: *Virus Bulletin* - January 1993 (p.12).

PRODUCT REVIEW 2

Dr Keith Jackson

PC Tools 8

The subject of my review this month, *PC Tools*, is the latest in a long line of versions of this software package. For the record, I first wrote about *PC Tools* over five years ago (not for *VB*), and it has come on a long way since then - not least in the amount of disk space required by the software. The original *PC Tools* fitted on to a single floppy disk, Version 8 comes on *five* compressed 1.44 Mbyte disks (3.5 inch, permanently write-protected), and when installed occupies over 8 Mbytes of hard disk space.

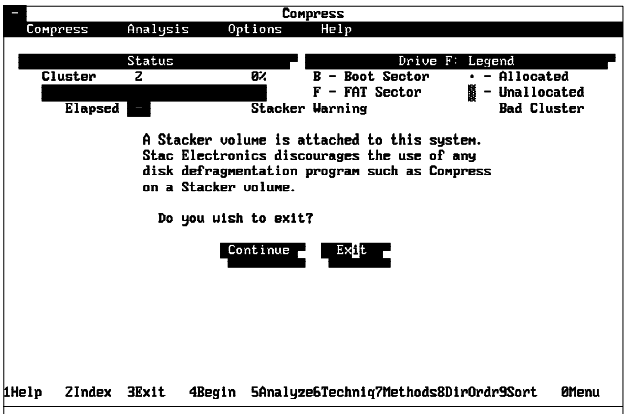
Component Parts

The software provides a host of facilities in one integrated package. Many versions ago, they were just individual 'tools' which had been bolted together, but since then the package has been given more cohesion, and has a comprehensive 'desktop' program which can be used to control just about anything.

A complete list of the available functionality is impossible in this short review, but just including those features that are relevant as far as dealing with viruses is concerned produces the following list - data recovery features, an emergency disk that can be used when all else fails, security programs that can help monitor unwanted introduction of files and aid in their removal, an anti-virus program which can detect, remove and immunise, memory-resident programs that monitor for virus activity, a backup program, and a scheduler that lets *PC Tools* programs (or any program, for that matter) operate at regular timed intervals. Bear in mind that this merely describes the facilities that are useful in fighting viruses, it ignores the notepad, outliner, calculator, database, fax, electronic mail facilities etc that are also included.

Given the breadth of coverage provided, I will concentrate on the facilities available from the components of *PC Tools* which are relevant to anybody having to deal with effects caused by computer viruses. These can range from detecting virus infections on floppy and hard disks, to repairing damage to hard disks which exhibit one of the myriad problems caused by viruses.

Central Point Anti-Virus (one component of *PC Tools*) was reviewed by *VB* in June 1991, and looked at again as recently as May 1992, but Version 8 of *PC Tools* is a major upgrade which well deserves looking at in its entirety.



For all its mammoth size, a great deal of attention to detail can be seen in the product. Here the software warns against a potentially dangerous operation.

PC Tools and *The Norton Utilities* compete for what is effectively the same market, and they have no other serious competition. *Norton Anti-Virus* was reviewed in the January 1991 edition of *VB*, and again in April 1992, but the compete *Norton Utilities* (as opposed to just the anti-virus part) has never been reviewed by *VB*.

Doorstop Documentation

In last month's review I spent some time complaining about the skimpiness of the documentation. *PC Tools* lies at the other extreme; it comes with two large bound volumes comprising nearly 1500 pages of *very* thorough documentation. It is well laid out, thoroughly indexed, and my only complaint is that one index refers to both volumes (using a slightly different typeface for each), so that I continually looked things up in the wrong book. However if the documentation had comprised 1500 pages in one enormous doorstop of a book, I suppose that I would have complained even more.

The first *VB* review of *Central Point Anti-Virus* stated that the documentation was a 'professionally produced work', but somewhat 'uninspiring', the next review stated that it had improved to 'very readable', and with Version 8 I am pleased to see that further development work has been put in and the documentation has improved even more. All this is coupled with on-line help, so the developers deserve ten out of ten for documentation.

Installation

Installing *PC Tools* proved to be very easy. The installation program firstly scanned memory for viruses, then detected that I had a colour video monitor, and offered various screen choices. The installation process can either be mouse driven or keyboard driven (as can all the *PC Tools* pro-

grams). A complete installation requires nearly *9 Mbytes* of hard disk space, but this can be reduced either by installing one of the preselected stripped down versions, or by using the custom installation option to decide for yourself which components are required. A de-installation option is proffered to the user but unfortunately this does not work too well. Although it removes the *PC Tools* executable programs, and other files in the same subdirectory, it leaves checksum files (.CPS) scattered throughout every directory of the hard disk.

The installation programs warns users not to install *PC Tools* while in the midst of trying to recover information from a damaged hard disk - after all, installing new software can overwrite the very files that need to be retrieved. Therefore even though most of the files are held in compressed form on the *PC Tools* floppy disks, the components which are required to execute from floppy disk are stored in uncompressed form. They will therefore operate directly from the floppy disk, albeit minus some of their features, such as on-line help.

During installation an 'Emergency Disk' can be created (on a blank floppy disk) which contains the requisite MS-DOS files to boot a computer, the DISKFIX program that is capable of repairing many disk problems, mouse drivers, the MS-DOS program FDISK for use when a hard disk has to be repartitioned, the *PC Tools* disk formatting program, and the UNDELETE and UNFORMAT utilities.

This is a comprehensive set of tools, although it should be noted that it takes up over a megabyte of disk space, and is therefore not much use on older PCs which have floppy disk drives with a smaller capacity. I was impressed that *PC Tools* even took note that I use the *Stacker* compression utility and copied the requisite software across to the Emergency Disk.

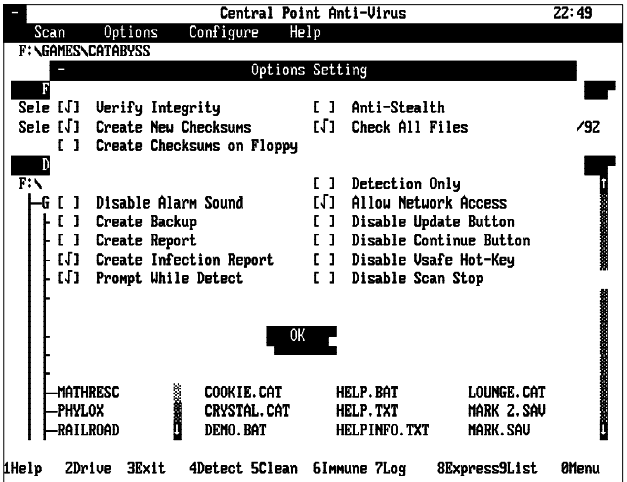
Virus-Specific Detection

As far as viruses are concerned with *PC Tools*, the main possibilities seem to be to detect whether a virus infection is present, remove any incidence of the infection, repair any damage caused to data stored on a disk (of any type), and restore files from backup if they are irretrievably damaged. I'll consider each of these aspects below.

The Central Point Anti-Virus software incorporated within *PC Tools* is seemingly identical to that distributed as a stand-alone package. The reader should refer to the complete *VB* review of this package mentioned above for comprehensive details of the available facilities, which have not changed substantially. However, the test set of viruses used for these reviews has been extended in recent months, so I retested the virus detection capabilities. *PC Tools* was capable of scanning my hard disk in 33 seconds, searching through 744 files occupying 10 Mbytes of disk space. For comparison purposes, *Dr Solomon's Anti-Virus Toolkit* performed the same test in 14 seconds, and *Sweep* from *Sophos* took 13 seconds in quick scan mode, and 53 seconds when doing a complete scan.

The accuracy of virus detection was quite good - *PC Tools* detected all except four of the 215 virus samples listed in the *Technical Details* section below (it missed Kamikaze, Rat and two copies of Amstrad). There were many instances of wrong naming of viruses which went beyond the nomenclature problems produced by many other scanner programs, as it really does seem to detect the wrong virus on occasions. Given the interlinked nature of many species of virus this is neither too surprising nor too worrying. Very impressively, all of the recently introduced test viruses were detected correctly, though rather curiously the omitted Amstrad virus samples were detected by previous versions of this program.

I tried to test the scanner against 1024 samples of the Groove virus, which is encrypted using the Mutation Engine. This proved impossible, as the package consistently locked up while running this test, and would not produce a report on file. After much effort I retrieved the unsaved file from the disk (using *PC Tools!*), and discovered that it detected 235 from the first 256 samples of the Mutation Engine (92%), and always locked up when exactly 255 viruses had been entered into the report. This is such a 'round number' that it is almost certainly a software bug. About half of the Groove virus infections were not denoted by this name but were identified as simply 'infected' with the Mutation Engine.



One of the principal criticisms of *Central Point Anti-Virus* was that it blindly recreated missing checksum files. This loophole has now been plugged.

Generic Detection

The last *VB* review of *Central Point Anti-Virus* complained that although it claimed to monitor file integrity using a 'checksum', this did not seem to be calculated across the entire file. Indeed tests showed that there was no possibility that the software was examining the entire file. The manual is still quite explicit on this point. It states that in each subdirectory there is 'a database of statistics, about each executable file size, attributes, date, time and a checksum'. There is still no mention of a checksumming algorithm, which makes it hard to take such a system seriously.

Other available anti-virus facilities are immunisation against viruses (against which I have railed in the past, so I will not repeat the arguments against this technique here), the capability of removing viruses from infected files (which seemed to work well), and several memory-resident utilities which attempt to detect virus activity during normal computer operation.

Disaster Recovery

The mainstay of *any* anti-virus strategy should always be frequent, tested, backups. The backup facilities offered by *PC Tools* are comprehensive to say the least, including data compression, password protection, encryption (to varying degrees of security), and on-the-fly virus detection. Back-ups can be written to floppy disk, a network drive, and a SCSI or a QIC tape drive. Various types of full or partial backup can be taken, and in common with the anti-virus features, backups can be organised by the scheduler program on a timed basis.

If the worst has happened and a virus has actually triggered, then other components of *PC Tools* come into their own, and provide comprehensive facilities to help ameliorate the consequent problems. Files, subdirectories, disks, disk sector(s), the boot sector or the FAT can be manipulated by an experienced user. Indeed it is possible to do almost anything to a hard disk drive, though like all powerful tools this must be used with due care and responsibility.

The COMMUTE program lets a user of one PC operate another PC either via a modem, across a network, or via a serial line. Most (all?) of the available programs have an Express menu system and a Full menu system. The former provides simple execution facilities, and the latter lets execution be tailored for a particular type of use. One helpful feature is that the transfer from Express menus to Full menus can be password protected, so an administrator can enforce a particular way of operation upon users.

Operation is possible either from DOS or from *Windows*, and the installation program creates a *Windows* group with an icon for every feature offered by *PC Tools*. However, I would advise that virus infections are best cleared up using DOS, rather than having a layer of *Windows* software insulate the user from direct access to the hardware.

Conclusions

Complaints about this month's product are few and far between. I do feel miffed at having to give up nearly 9 Mbytes of precious disk space, but if vendors wish to cater for all possibilities, then size inevitably becomes a problem. Keeping programs small enough so that they can be executed directly from a floppy disk is the real problem, as this is *essential* when dealing with viruses. *PC Tools* can only just do this, and already inherently assumes that a high capacity floppy disk is available.

The virus detection report really should not lock up so thoroughly that it does not leave behind an intact report file, after all, an infected hard disk may well contain more than 255 infected files. Leaving behind umpteen checksum files scattered in every subdirectory of a hard disk after *PC Tools* has been de-installed may well have been a design decision taken to facilitate software upgrades, but I found myself becoming irritated at having to clear them all out manually.

It is my firm belief that anyone who has to deal with virus outbreaks needs to purchase one or other of *The Norton Utilities* or *PC Tools*, but I don't think it really matters which one is chosen. Personally I use *Norton*, but that is more a matter of history than logic, as I was introduced to Peter Norton's programs first. If I had come across *PC Tools* first then I may well have taken the inverse choice. If you don't own a copy of at least one of them, then one day you'll find out why you should.

Technical Details

Product: *PC Tools* version 8

Developer: Central Point Software Inc., 15220 NW Greenbrier Parkway, #200/Beaverton, OR 97006, USA, Tel: +1 (503) 690-8080, BBS: +1 (503) 690-6650, and +44 (81) 569-3324.

Vendor(s): Available from most computer dealers.

Availability: IBM PS/2, PC, XT, AT and most IBM compatible computers, with DOS v3.3 (or later), 512 Kbytes of RAM (640 Kbytes recommended), 1 floppy disk drive and 1 hard disk drive.

Version evaluated: 8

Serial number: None visible

Price: £139 +VAT

Hardware used: (a) 33MHz 486 PC, with one 3.5 inch (1.44M) floppy disk drive, one 5.25 inch (1.2M) floppy disk drive, and a 120 Mbyte hard disk, running under MS-DOS v5.0. (b) 4.77MHz 8088, with one 3.5 inch (720K) floppy disk drive, two 5.25 inch (360K) floppy disk drives, and a 32 Mbyte hardcard, running under MS-DOS v3.30. For details of the viruses used for testing purposes see *Virus Bulletin*, December 1992, p.22.

END-NOTES AND NEWS

Problems have been reported by users of *Norton Desktop for Windows*, which result in damaged data. The product, which includes an anti-virus element, is reported to cause file corruption and system instability under certain conditions. (File corruption may, however, be repaired using *PC Tools*. See p.21.) For further information contact *Symantec*. Tel. 0628 592222.

Datawatch has upgraded its anti-virus product, *Virex-PC*, to make it more *NetWare* and *Windows* aware. The product is now capable of sending virus alerts to *Novell NetWare* consoles. Tel. +1 (919) 490 1277.

The ***NETSEC '93*** conference, Network Security in the Open Environment, will be held on June 21-23, 1993 at the *Capital Hilton*, Washington. For further information, contact the *Computer Security Institute*. Tel +1 (415) 905 2310.

Graphnet Computers has been appointed as the sole UK agent for *V-BUSTER*, a product which will 'detect and inactivate a total of 1494 named viruses, as well as virtually all unknown ones.' The software, written by *Looi Software* of Penang, Malaysia, costs £99 + VAT. It has not been reviewed by *Virus Bulletin*, however, as it is only sold in copy-protected form. Tel. 0278 663680.

An infamous hacker has been charged with stealing ***United States Air Force*** secrets. Kevin Poulsen, who was accused in the early 1980s in a landmark hacking case, faces between seven and ten years in prison if convicted. He has allegedly stolen classified information, including a list of *USAF* targets in a hypothetical war.

The **Dutch Police's computer crime squad** has reported a doubling in the number of cases it has to handle. In a nine month period in 1992 the unit recorded 67 cases, compared to 33 for the same times last year. Frans van Gulik, commander of the Hague squad, commented that open systems and networking were increasing the opportunities open to criminals.

Gareth Hardy, a former computer manager, **has admitted planting a logic bomb in his employers system**, according to a report in *Computer Weekly*. Hardy was employed by *Chilworth Communications* in July 1990, and following a number of warnings handed in his notice on 2nd September 1991. After this, he installed a logic bomb which encrypted a number of vital files one month after he left the company. In court, Hardy admitted to unlawfully making modifications to computer material, contrary to section 3 of the *Computer Misuse Act*. He was sentenced to 140 hours community service, and ordered to pay £3000 compensation.

***ASP* has announced** that as from January 1st, it is to transfer all maintenance, marketing and other responsibility for all information protection products currently made and marketed by *ASP* to outside companies in which *ASP* has no commercial interest. This transfer has been done so that *ASP* cannot be accused of a conflict of interest in its new joint venture with Information Integrity. The new project, *Protection Experts*, aims to provide on-line technical advice on computer security issues - charged at $3 a minute ('just putting you on hold sir...'). For free information contact ASP. Tel. +1 (412) 422 4134.

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