ISSN 0956-9979 JANUARY 1994

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

Editor: **Richard Ford**

Technical Editor: **Fridrik Skulason**

Consulting Editor: **Edward Wilding**, Network Security Management, UK

IN THIS ISSUE:

• **Scanners galore.** Just how well are the scanner manufacturers keeping up with the steady influx of new viruses? Nineteen different products are put through their paces on pages 14-19.

• **Cyber Riot.** The first virus which takes full advantage of the additional functionality provided by *Windows* is here. What are the implications?

• **Forbidden Subjects.** Several different CD-ROMs have been found to contain virus code - including one where the code was intentionally written to the disk. The risk of infection from this medium seems to be increasing.

CONTENTS

EDITORIAL
Washes Whiter 2

VIRUS PREVALENCE TABLE 3

NEWS
CD-ROM Virus Bonanza 3
Virus Bulletin '94 3

IBM PC VIRUSES (UPDATE) 4

INSIGHT
Vesselin's World of Viruses 6

VIRUS ANALYSES
1. Barrotes: Wilful Damage 8
2. AVV - The Anti-Virus Virus 10
3. Riotous Assembly 12

COMPARATIVE REVIEW
1994 Scanner Test 14

PRODUCT REVIEW
Blue-Blooded DOS 20

FEATURE
That was the Year 23

END NOTES & NEWS 24

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

EDITORIAL

Washes Whiter

No doubt everyone has their own favourite television or cinema advert - possibly the *Coke* commercials featuring 'Vicars who surf' or a plug for a favourite beer spring to mind. In most cases, these adverts are aimed at either associating a particular image with a product or (just as importantly in marketing terms) simply 'getting the name out'. In a tightly squeezed market, good advertising can make the difference between success and failure. Nowhere is this more true than in the highly competitive anti-virus industry.

As an interesting experiment, *Virus Bulletin* (posing as a prospective customer) requested further information from several companies which market anti-virus software. The response ranged from receiving no reply at all (the guilty company will not be named, in order to protect its sales staff!) to being sent a fully working copy of the product.

"If all anti-virus products are equal, some products are more equal than others"

The first step towards making a sale is to generate the initial enquiry. This is most often done through advertisements in the computer press, as well as via direct mail campaigns. Most people will doubtless remember the early *S&S International* advert, which pictured a 5.25-inch disk spattered with egg, under the headline 'Most computer vandalism is not this easy to spot'. Excellent, eye-catching and effective.

However, the *VB* prize for the most memorable advert has to be awarded to *Total Control*. Featuring two floppy disks (one pink, one blue) reclining in a bed, the poster led with the caption 'Before you put it in… make sure you know where it's been'. The advert was banned almost immediately after release. Back to the drawing board…

When a company has converted a 'suspect' to a 'prospect' (to use marketing jargon), it must then convince the user that its product offers something which others do not. For example, *IBM* attempts to push the 'consultancy' aspects of its service, showing the reader that support and expertise is just as important as software, whereas *Symantec* uses the Peter Norton name and image to sell *NAV*. The *S&S* sales pitch is very much more focused. The advertising style of the company has always been hard-hitting and to the point. '*Dr Solomon's* range of *Anti-Virus Toolkits* provides the answer in almost every situation', readers are informed in a saccharin-sweet leaflet. This aside, the advertisement informs without making too many excessive claims.

Intel's information pack consists of a pastel green flyer and a 'Test Drive Kit' - the 'try before you buy' approach. The flyer informs readers that *Intel LANDesk™* is the 'Industry's most advanced detection technology'. Something is awry here: *Norton Anti-virus* is (according to its flyer) 'The Best Defence'. However, *Central Point* is 'the only … product to provide true global virus management.' In fact, just about every package is either 'unrivalled', 'the most advanced' or 'the best'.

The problem is that going by the adverts alone leaves one little or no idea about which product is the most suitable for a particular site. The only way to make an unbiased, objective decision is to evaluate product performance. Sadly (or, for some companies, fortunately), most users can only evaluate the look and feel of the software, not how well it actually works. Buyers are thus saved the 'doorstep challenge' type of marketing ('We scanned this disk with *Acme VirKill Plus*, and this disk with another top virus scanner…') - but the most important parts of the product go untried.

If all anti-virus products are equal, some products are more equal than others. One needs only to glance at the results of this month's comparative review to see that certain packages consistently perform better than others. Purchasing a good virus scanner is still a hit and miss affair: the overall standard of anti-virus software has vastly improved over the last few years, but there are still a few products which are poor value for money. Although performance is not the only criterion for choosing a product, it must be remembered that the purpose of anti-virus software is to detect viruses, not to look pretty. The most important facts about each product are shown on page 15. These figures are the *only* way to tell which product 'washes whiter'. Happy shopping.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

NEWS

CD-ROM Virus Bonanza

December was a particularly bad month for viruses on CD-ROM. Four different incidents have been reported, and users would be well advised to ensure that CD-ROMs are scanned just like any other incoming disk. This process is further complicated by the large number of compressed files that such CDs are likely to contain.

The only CD so far published which deliberately contains virus code is produced by *Profit Press*. The CD is called *Forbidden Subjects*, and claims to contain information on hacking, phreaking, and virus code, in addition to a long list of other assorted subjects. However, it is no cause for alarm, as although it does contain the source code to some simple viruses, most of the information on PC viruses is contained in a number of back issues of *40Hex*. Copies of these files are already freely available via anonymous ftp from a number of Internet sites.

The two shareware CDs reportedly infected with viruses are cause for concern. The first of the two, *Software Vault, Collection 2* is published by *American Databank Corp*, USA, and according to a report in the *F-Prot 2.10 Update Bulletin*, is infected with the PS-MPC.Math-test virus.

This virus activates between 9:00am and 10:00am every day, requiring the user to enter the answer to a simple mathematical problem before he is allowed to execute any other program. The infected file is located in the directory '18' of the CD-ROM, inside the zipped file 64BLAZER.ZIP.

The second CD-ROM is *Night Owl #10*, which contains a file infected with the Lapse virus. This is a simple EXE file infector, written in Canada. The virus does not contain a trigger routine, and is not capable of remaining memory-resident. The infected file is located in the 'Games' directory in the file SF2_UP.ZIP.

According to a report published by *F-Prot* distributor, *Data Fellows*, both manufacturers admit the infections, and the CDs will probably be withdrawn.

In a separate incident, *Apple Sweden* sent out an alert, concerning the Merryxmas virus, which was believed to be present on a CD-ROM, shipped to all *Apple* distributors. Dealers in most Nordic countries were warned about the virus, and instructed not to copy files from the CD.

While investigating the story, *Virus Bulletin* discovered that the CDs were not infected, and that the alert was simply the result of a false positive. *Apple Sweden* was notified, and the alert has now been dropped. However, the incident highlights both the need to scan all software from CD-ROMs, and the confusion which can be caused by a false positive. The principal problem with an infected CD is that the file cannot be deleted; the entire CD must be destroyed▮

Virus Prevalence Table - November 1993

Virus	Incidents	(%) Reports
Form	21	43.8%
New Zealand 2	6	12.5%
Cascade	3	6.3%
V-Sign	3	6.3%
Helloween	2	4.2%
NoInt	2	4.2%
Parity Boot B	2	4.2%
Dir II	1	2.1%
Eddie 2	1	2.1%
Exebug	1	2.1%
Maltese Amoeba	1	2.1%
Piter	1	2.1%
Spanish Trojan	1	2.1%
Stoned-O	1	2.1%
Tequila	1	2.1%
Yankee.2C	1	2.1%
Total	48	100.0%

Virus Bulletin '94

The 1994 *Virus Bulletin Conference* is set to return to its birthplace: the conference will be held on September 8th and 9th at the *Hôtel de France*, Jersey. Last year's *VB Conference* in Amsterdam attracted delegates and speakers from over 25 countries, making it the biggest and best European gathering of anti-virus experts in 1993.

Speakers at previous *Virus Bulletin* conferences have included Fridrik Skulason, Fred Cohen, Vesselin Bontchev and Steve White. However, the conference is far more than just a gathering of virus researchers. The programme is of immediate relevance to anyone who is responsible for virus prevention within their organisation.

The 1994 conference promises to be different from its predecessors, both in content and in cost. Not only is the registration fee lower than in 1993, but the overall cost of attendance has dropped: a complete package including registration, a flight from London and two nights' accommodation will cost under £800.00.

For the first time, the *VB Conference* will feature an exhibition by anti-virus product vendors, providing delegates with an unparalleled opportunity to discuss their requirements with the major suppliers.

For details on the conference and the exhibition, please contact Petra Duffield on Tel. +44 (0)235 531889 or Fax +44 (0)235 559935▮

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

IBM PC VIRUSES (UPDATE)

The following is a list of updates and amendments to the *Virus Bulletin Table of Known IBM PC Viruses* as of 10th December 1993. Each entry consists of the virus name, its aliases (if any) and the virus type. This isfollowed 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 a dedicated scanner which contains a user-updatable pattern library.

Type Codes

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

Arriba.B **CER:** A minor variant, detected with the Arriba pattern.

Baobab.2304 **ER:** Very similar to the 1635-byte variant. Detected with the Baobab pattern.

Barrotes.1310 **CER:** Several new 1310-byte variants (B, C, D, E and F) have been reported, but they are all detected with the Barrotes pattern.

Better World.B **ER:** Very similar to the A variant. Detected with the Better World (Fellowship) pattern.

Bupt.1220.B **CER:** This virus is almost identical to Bupt.1220.A, except that a text message at the end has been partially overwritten. Detected with the Bupt (Traveller) search pattern.

Dark Apocalypse **CEN:** A 1020-byte virus which activates on Monday 10th (any month), overwriting critical parts of the hard disk.

```
Dark Apocalypse B42A CD21 3C01 7528 80FA 1075 23B4 19CD 218D 9EBB 02B9 0100
```

Dark Avenger.1800.J **CER:** A minor variant, detected with the Dark Avenger pattern.

Deicide.665 **CN:** This overwriting virus is a minor variant of the original Deicide virus, but one byte shorter. It is detected with the Deicide pattern.

Deicide II.2569 **CN:** Very similar to the Commentator viruses reported in December 1992, but has a different length.

```
Deicide II.2569 B440 BA00 01B9 EE09 CD21 B457 B001 5A59 CD21 B43E CD21 8B1E
```

Du **ER:** A 725-byte virus. Awaiting analysis.

```
Du              B8F0 FACD 213D DDDD 7503 E9AC 001E 33C0 8ED8 A164 008B 1E66
```

Freew.718.B **CN:** Detected by the pattern provided for the A variant, which was originally named 'Bob'.

Friday the 13th.417 **CN:** This variant might have been created from the same source as the 416-byte version, but using a different assembler. Detected with the Friday the 13th (formerly called South African) pattern.

Gergana.182.B **CN:** A minor variant, detected with the Gergana pattern.

Hi.895 **ER:** This is a new variant of the Hi virus, which was originally reported in August 1992. This 895-byte long sample is much shorter than the original. Detected with the Hi pattern.

Infector **CN:** Four new variants of the Infector virus are now known.

```
Infector.676    A200 01A0 2F03 2EA2 0101 A030 032E A202 01B9 8000 BB00 002E
Infector.759    A200 01A0 DC02 2EA2 0101 A0DD 022E A202 01B9 0001 BB00 002E
Infector.822.B  A200 01A0 8703 2EA2 0101 A088 032E A202 018C C8A3 3603 B980
Infector.962    A200 01A0 A503 2EA2 0101 A0A6 032E A202 01B9 0001 BB00 002E
```

Internal.1459 **ER:** A 1459-byte virus. Awaiting analysis.

```
Internal.1459   1E06 8CC8 8ED8 B840 008E C0FC E8A6 0480 3EAF 0000 740B E8C1
```

Kernel **CR:** This 608-byte virus was named after the word 'KERNEL' it contains, but it also contains another, encrypted text string: 'Dedicated to tfe 13021 lost sheep. Please God, do help them. !!' (sic).

```
Kernel           9C80 FC4B 7403 9DEB EE50 5351 0656 571E 52B4 04CD 1A81 FA08
```

Knight **CN:** An encrypted, 1136-byte overwriting virus, which contains the string '-KNIGHT-'.

```
Knight           8B1C 31D8 8905 4681 FE11 0175 03BE 0701 81C7 0200 81FF 7005
```

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

Leprosy **CN/EN:** Several new variants of this family of overwriting viruses have been reported recently: Leprosy.Fratricide (CEN, 647 bytes), Leprosy.Clinton (EN, 654 bytes), Leprosy.H (CN, 666 bytes), Leprosy.Surfer (EN,946 bytes) and Leprosy.5600 (EN, 5600 bytes). The Clinton variant is detected with the standard Leprosy pattern.

```
Fratricide      8B1E 3D02 53E8 1400 905B B987 0290 90BA 0001 90B4 4090 CD21
Leprosy.H       8B1E 6E01 FA53 FBE8 1600 905B FBB4 40FA BA00 01FA B99A 02FB
Leprosy.Surfer  A127 0350 E80F 005B B9B2 03BA 0001 B440 CD21 E801 00C3 BB30
Leprosy.5600    8B1E 8101 9053 90E8 1500 905B 90B9 E015 90BA 0001 90B4 4090
```

Little Girl.949, Little Girl.985 CER: Two new variants, both detectable with the Little Girl pattern.

Manuel **CR:** Nine new variants of this virus have been reported recently. They are 777, 814, 840, 858, 876, 937, 995, 1155 and 1388 bytes long. None of them are detected with the Manuel search pattern.

```
Manuel (2)      F9C3 A675 FBF8 C3FC 268A 2547 AC3C 0074 143A C475 F757 56E8
```

March 25th **CER:** This virus is probably of Italian origin. It activates on March 25th, trashing the hard disk.

```
March 25th      80FC 3074 2D3D 003D 7428 3D00 4B74 232E FF2E 3200 B42A CD21
```

Mel **EN:** A 1536-byte Polish virus. Awaiting analysis. The name is derived from a text string the virus contains: 'All in All, You are just another BRICK in the WALL (MEL)'. The virus contains other text strings as well, including the following message in Polish: 'Wirus calkowicie nieszkodliwy, jak jestes enough dobry to napisz szczepionke'.

Milan.WWT.67.C, Milan.WWT.125.C CN: The WWT viruses have now been re-classified as members of the Milan family. They are primitive overwriting viruses, 67 and 125 bytes long. The new variants have been modified slightly, probably to avoid detection by some scanner.

```
WWT.67.C        B901 00BA 3D01 B44E CD21 7302 EB1E B802 3DBA 9E00 CD21 7302
WWT.125.C       B901 00B4 4EBA 7101 CD21 7302 EB10 E80F 00B4 4FBA 8200 CD21
```

MPS-OPC.754 **CER:** A Polish virus, detected with the MPS-OPC 4.01 pattern.

Mr. D **ER:** This is another Polish virus, 1536 bytes long. Two variants are known (A and B), but they are both detected with the following pattern. Disinfecting the virus is a problem, as it does not preserve the original SS register value.

```
Mr. D           9C3D 004B 7539 2E8C 1638 002E 8926 3600 BCA1 052E 8E16 3A00
```

Mr. G.314 **CN:** This 314-byte virus seems to be an improved version of the 253-byte virus reported in June.

```
Mr. G.314       03FE 8BF7 CD21 5EBA 3B02 03D6 B44E 33C9 CD21 B801 43BA 9E00
```

Murphy.Amilia.B, Murphy.Swami.B CER: Similar to the A variant, and detected with the HIV pattern.

Murphy.Tormentor.E **CER:** This 1072-byte variant is very similar to the Murphy.Tormentor.B virus, and is detected with the HIV pattern.

Nina.D **CR:** This is a Swedish variant which was posted on FidoNet recently. According to the documentation it was modified to bypass *SCAN* and *Dr Solomon's Anti-Virus Toolkit*. Detected with the Nina pattern.

Npox.963.B **CER:** A minor variant, detected with the Npox and Npox.900 (previously named ZK-900) patterns.

Old Yankee.Enigma.B, Old Yankee.Enigma.C ER: Similar to the A variant, and detected with the Old Yankee pattern.

Protect.1323 **CER:** 1323 bytes long, and detected with the Protect pattern.

Prudents.B, Prudents.C **ER:** Similar to the A variant, and detected with the Prudents pattern.

Quit-1992.B **CER:** Detected with the Quit-1992 (previously named 555) pattern.

Red Diavolyata.830.D **CR:** This is the 'SUPER.EXE' sample from the Part1.ZIP collection discussed last month. Detected with the Red Diavolyata (MLTI) pattern.

Seventh Son.428 **CN:** This virus was posted on FidoNet by a member of a Swedish virus-writing group. It contains the string 'ARBEIT MACHT FREI!'. Detected with the Seventh Son pattern.

Storm.1217 **CR:** Yet another variant of this virus, 1217 bytes long.

```
Storm.1217      FA9C 3D00 4B74 143D FE4B 9075 07BD 3412 909D FBCF 9DFB 2EFF
```

Troi.B **CR:** Similar to the A variant, and detected with the Troi pattern.

Vienna.645.C, Vienna.645.D **CN:** Two minor variants, 645 bytes long. The C variant is detected with the GhostBalls and Vienna.1239 patterns, but the D variant is detected with the Vienna (1) and Dr. Q patterns.

Zamoy **CN:** This is a 587-byte Polish virus. Awaiting analysis.

```
Zamoy           817D FD4F 4D75 BC2E 8B3E 0601 8B76 0081 C68C 0203 F781 7C1A
```

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

INSIGHT

Vesselin's World of Viruses

Megan Palfrey

Bulgaria, alleged virus capital of the world! When a country has such a reputation, it is hardly surprising that it also boasts one of the world's foremost anti-virus researchers, Vesselin Vladimirov Bontchev.

Working it Out

Bontchev's interest in computers was kindled by FORTRAN, the language his mother used in her work at the *Bulgarian Academy of Sciences*. As a teenager, he asked her to write a program for him, to make a board game he was playing easier. She gave him the FORTRAN manual and told him to do it himself. 'So,' he says, 'I did!'

This pastime soon became a consuming fascination in seeing a machine perform tasks for which the presence of human intelligence is intuitively assumed: 'One feels that one is controlling another intellect,' explains Bontchev. 'If it does something wrong, it is one's own mistake and is correctable, not something based on a bad mood, or because it doesn't like you. I like deterministic things, things I can control.'

Getting There

Bontchev decided to study computer science, but was first obliged to do two years' National Service in the army. This did little to dull his enthusiasm for computers, however. After gaining his degree from the *Technical University* in Sofia, he worked in their laboratories for a year before taking up a post at the *Institute of Industrial Cybernetics and Robotics* in the *Bulgarian Academy of Sciences*. During his time there, he also did freelance work for the magazine *Komputar za Vas* (*Computer for You*)… and by pure chance, encountered his first virus.

One of his commissions was to correct a paper on computer viruses, which had been translated from German by a non-technical interpreter. This understandably led to interesting mistranslations: for example, the German for hard disk - 'Festplatte' - was translated as 'hard plate'! This was Bontchev's first foray into the world of computer viruses, and the phenomenon rapidly absorbed him.

He spent considerable time researching the subject, reading everything he could obtain ('there wasn't that much available at that time'), and eventually decided that viruses, despite being a thought-provoking concept, were neither an immediate danger nor a real threat. 'I even published a paper on the subject, explaining why,' laughs Bontchev. 'What I failed to consider was that not every user is a system hacker. Most users have little or no idea about what happens inside their computers.'

The Virus Takes Hold

Soon after publication of that article, two programmers came into the offices of *Komputar za Vas*, claiming to have discovered a virus. In demonstrating their disinfection program, they eradicated their only copy of the virus (having already disinfected their office system), leaving themselves with just a paper with the hex dump of an infected file written on it. This enabled Bontchev to enter the virus code byte by byte, and to disassemble his first real virus: Vienna.

As viruses became more widespread, and his involvement in the area grew, Bontchev wrote articles on viruses and anti-virus software. 'Most people considered computer viruses to be some kind of black magic,' he says, 'but it was interesting to me, and I discovered that I was quite good in handling virus problems.' It was not long before he became recognised as an expert in the field.

Epidemic or Exaggeration?

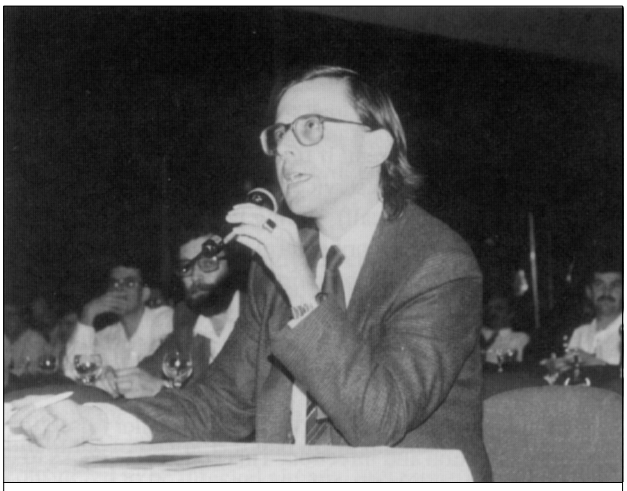
Bontchev becomes rather annoyed when Bulgaria's prolific virus output is mentioned: 'The truth is that a significant part (about ten percent) of existing viruses have been created in Bulgaria, and many of the novel ideas in virus writing were first invented and tried out there. The media report this as "the deadly computer viruses are coming from Bulgaria". It is true that lots of viruses have been written in Bulgaria, but most have remained there - only a few have been exported! Furthermore, there are many other countries very active in virus writing - Russia, USA, the Netherlands, Italy, to name just a few. Some of them, such as Russia and the USA, have created more viruses than Bulgaria.'

> *"Long-term problems are caused not by polymorphic viruses, but by the sheer number of viruses around"*

In Bontchev's opinion, there are a number of factors which contribute to the 'popularity' and pervasiveness of virus activity in Bulgaria. Possibly the principal cause is the large number of disillusioned young programmers who live there: they are undervalued and underpaid, in some cases earning as much as 100 to 120 *times* less than their American counterparts. Bontchev sees the step from embittered young programmer to virus writer as a small one.

He believes there are also other influences on the rampant spread of virus-writing in Bulgaria: the presence of a virus exchange BBS, software piracy, lack of software copyright laws, and lack of legislation against creation and wilful distribution of viruses, to name but a few.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.



Bontchev: 'When a new virus appears - and this could reach dozens per day - no-one will know whether this is new or just "not yet classified", and scanners will become useless.'

The most famous (or infamous) of the Bulgarian virus authors is the Dark Avenger, whose 'creations' have spread far and wide from their origins. Bontchev has little regard for the person hiding behind this pompous *nom de plume*, viewing him as a troublemaker: 'He has caused a lot of trouble with his MtE and Commander Bomber. If he manages to combine both ideas - a virus with the infection strategy of Commander Bomber and the polymorphism of MtE-based viruses… I wouldn't know how to make a scanner which could detect such a virus.'

The Dark Avenger has produced nothing new in the past year-and-a-half, and, according to Sara Gordon (who claims to have interviewed him), he has given up virus writing. Although Bontchev has suspicions as to the Dark Avenger's identity, he refuses to commit himself: 'Clues I do have, but not enough to point to a particular person "beyond reasonable doubt" - that's why I say that I don't know who he is.'

Into the Crystal Ball

I asked Bontchev where he saw the virus issue leading: his response was that viruses may soon be innumerable. 'When a new virus appears - and this could reach dozens per day - no-one will know whether this is new or just "not yet classified", and scanners will become useless.' He feels that anti-virus techniques must evolve, and that the integrated system will triumph. This might consist of components such as an heuristic analyser, a memory-resident scanner, a Network Loadable Module, and some sort of integrity checker, in addition to an off-line scanner.

'The integrity checker will probably be both resident and off-line, and will be able to identify and analyse modifications in executables. If they appear to be caused by a virus, it will restore the executable to its original state. There will be integrity checking of system memory, to ensure that no viruses are memory-resident. In addition, future products will be able to restore the whole operating system to a known clean state before continuing with further checks.

'Polymorphic viruses will be dealt with generically. *Dr Solomon's Generic Decryption Engine*, for example, decrypts an encrypted virus using the virus' own decryption algorithm. It can then be detected with a scan string.' However, this latest refinement merely represents the rising escalation of anti-virus warfare: 'Undoubtedly, as other anti-virus vendors develop more sophisticated products, virus authors will do likewise. Fortunately, most virus authors are merely hobbyists, with bright ideas but no basic knowledge.'

He views the future as bleak. 'Long-term problems are caused not by polymorphic viruses, but by the sheer number of viruses around. How many will a scanner be able to handle? 5,000? 10,000? 100,000? And, even if your scanner can handle 100,000 scan strings, would it be possible to extract as many as 500 scan strings per day? How much space will just the names of those 100,000 viruses take?'

Bontchev shares the widely-held belief that computer viruses will soon become a common ailment. He foresees standard systems with some built-in protection, and security products which will be able to stop most viruses, or at least contain the damage caused by an attack. One day, there will be specialists whose prime function will be providing 'anti-dotes' in the event of an infection. He believes it is also conceivable that insurance policies might become available to compensate for irrecoverable data loss, the premium based on how anti-virus measures are implemented.

The Best of All Worlds

Bontchev views no single product currently available as the 'best' anti-virus weapon, but points out that each has its own strengths and weaknesses: 'I would hate to advertise for anybody, but imagine an integrated product with an integrity checker as strong as *Untouchable*, a scanner that does exact identification as well as *Dr Solomon's Anti-Virus Toolkit*, detects variants of the known viruses as well as *F-Prot*, has heuristics as strong as *F-Prot* and *TbScan*, but with as few false positives as the *CPAV* heuristics, has an integrity shell as secure as *ASP*, is as unobtrusive as *IBM Antivirus*, has the nice user interface of *CPAV*, is as fast as *TbScan*, comes in *DOS/Windows/OS2*/NLM versions, and is as cheap as *F-Prot*. Well, that would be close to ideal…'

Bontchev firmly believes that prevention is better than cure. Top on his list of priorities are regular backups, but other things are also vital: one should learn how to remove DOS and Master Boot Sector viruses using SYS and FDISK, and boot only from the hard disk. Adhering to these simple rules would, in Bontchev's opinion, go a long way towards minimising the problem.

'Remember, computer viruses are not some kind of black magic created by computer geniuses, but small, nasty, buggy programs, written mostly by ignorant kids showing off,' states Bontchev. 'Support local legislation; insist that it passes laws against virus authors and intentional distributors. Finally, if you have knowledge that can help other people, share it, don't keep it to yourself.'

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

VIRUS ANALYSIS 1

Barrotes: Wilful Damage

Jim Bates

A recent survey on virus activity (*Virus Bulletin*, December 1993, pp.15-16) showed that most virus infections are caused by a handful of well-known viruses. This is most likely due to an increased level of user awareness, which prevents the majority of new viruses from becoming widespread. Aside from the obvious benefit, this means that if a new virus is discovered in the wild, there is a better chance of being able to establish where the virus was introduced.

The decrepitude of most viruses found in the wild bears no relation to the effort expended by virus authors; quite the contrary. Broadly speaking, most virus writers fall into three main groups - the 'demo virus' writer, the so-called 'researcher', claiming to advance virus knowledge, and the malicious author. The last group is by far the largest, and is unfortunately the most likely to try to get their code into the wild. Most new viruses are disseminated, via virus exchange BBSs etc, to an ever-increasing army of 'magpie' researchers. Continuing 'one-upmanship' (I have, I find, I know about more viruses than you) only serves to spread new viruses to a continually growing audience. The vast majority of samples, however, exist only as part of virus collections, and never actually spread to users' machines.

Barrotes (which means 'bars' in Spanish) is an exception to this rule. The virus has been passed between researchers for many months, but has only recently begun to become common in the wild. The virus contains a malicious trigger routine which attempts to draw bars on the screen while overwriting the MBS of the first fixed disk.

Overview and Installation

Barrotes is a memory-resident, parasitic virus, capable of infecting both EXE and COM files (including COMMAND.COM). It writes copies of itself to the end of suitable executable files, and modifies the code entry point to ensure immediate execution when the file is loaded. The virus contains a destructive trigger routine which attempts to overwrite the Master Boot Sector on January 5th of any year. During this process it also displays its name, so the user knows what has caused his loss of data. Barrotes does not attempt stealth or polymorphism, and therefore poses no detection problems whatsoever.

When executed, the virus code sets an index to establish its relative position in memory. An 'Are you there?' call (which consists of placing a value of EEh into the AH register and issuing an Int 21h function request) is then issued to determine whether the virus is already resident and active in memory. The virus is assumed to be memory-resident if the value FEh is returned in the AL register, and processing returns to the host program. If the call is unanswered, the virus collects the Int 21h service routine address (using the standard DOS function call), storing it within the virus code. The host program's memory control area is interrogated to locate the top of available memory and the virus code is moved up into it. Next, processing sets a register to point to C:\COMMAND.COM, and a marker to indicate that this is the installation phase of the code.

Execution now passes to that code in high memory used for system interception and infection. This code first checks to see if the installation flag is set, and if so, processing passes to the start of the trigger routine. This clears the flag and completes the virus installation, hooking the Int 21h vector. Once this process is complete, the date is checked: if it is January 5th, the trigger routine activates - otherwise, processing returns to the host program.

Operation

When memory-resident, Barrotes intercepts only two Int 21h subfunctions, EEh (used for the 'Are you there?' call) and 4B00h, the DOS Load_and_Execute call. This allows the virus to infect all files which are executed after it has become memory-resident. In an attempt to ensure that the virus is always active, however, the virus author deliberately invokes the infection process with the target filename set to C:\COMMAND.COM.

"The decrepitude of most viruses found in the wild bears no relation to the effort expended by virus authors"

The infection routine first checks that there is enough space on the target drive for the virus code. If not, the routine aborts to the original function request. If there is sufficient disk space, the virus hooks the DOS Critical Error Handler (Int 24h), in order to prevent any DOS error messages being displayed during the infection process. Before infection, the virus stores the target file's date and time stamps and attributes: these are all reset at the end of the infection routine. The file is then opened, and the first two bytes are read and checked to see if they are the 'MZ' marker, which specifies an EXE file.

If these two bytes are not present, the file is assumed to be a COM file, and the infection process begins in earnest. The target file is checked to ensure that its length lies between 254 and 64,000 bytes, and the last two bytes of the file are checked to see whether or not they are 'SO', the virus' own infection marker. If either of these tests fails, the routine aborts and allows the original Int 21h call through.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

Once the virus has ascertained that the target file is a suitable candidate for infection, Barrotes simply appends its code to file. The first three bytes of the host file are stored, and a jump to the virus code is inserted in their place. When this process is complete, the host file's original attributes, time and date stamp are replaced. Only then is the original Int 21h call allowed to complete.

EXE files are treated slightly differently. The last two bytes of the file are checked for the 'SO' indicator: if it is not found, the next process completes a similar check, 816 bytes before the end of the file. It is unclear why this is necessary, but the code seems to indicate an attempt to circumvent a problem the writer may have encountered with a particular file. If the indicator is found in either position, the file is considered to be infected already, and processing aborts. Otherwise, infection is similar to COM files: virus code is appended and the file header modified, to ensure that the virus code is executed first.

There is no apparent limitation to the size of EXE files infected, although there are some rudimentary checks to ensure that the image size and the file size match (ensuring that hybrid files containing additional resource or overlay elements are not infected).

The Trigger

The check for the trigger date is made only when the virus is first invoked. Therefore if an infected machine is switched on (and the virus becomes resident) before that date and left running until after January 5th, the virus will not trigger. The routine itself is simple: a handler routine for Int 1Ch (the system clock) is installed, and garbage data is written to the MBS of the first fixed drive.

The machine will continue to function after this, but the Int 1Ch routine will overwrite the screen with the message

```
Virus BARROTES pro OSoft
```

together with a series of multicoloured bars across the screen, as if it were viewed through a barred window. The colours cycle rapidly through the available range. Once the machine is switched off, there is no easy way of rebooting to access the data, since basic information about the disk structure will have been destroyed. However, since the data itself will be untouched, recovery is relatively painless.

Standard methods of virus protection apply to this specimen. An 'Are you there?' call can be duplicated to detect whether the virus is resident and active. For specific identification in files or memory, a simple pattern recognition sequence is enough, and can be incorporated into most basic scanning engines. Alternatively, a check might be made for the 'SO' marker, but such a short recognition string, even given the known offset at the end of the file, could lead to false positives. Since the code at this point is very specific, it is acceptable to use a longer pattern located at the end of the file. However, the possibility of its existence at a different location in EXE files needs careful consideration.

As Barrotes uses no stealth features, it is easy to detect generically. Any integrity checking software which completes a simple 'top and tail' check of program files will instantly recognise the addition of such code, whether or not the virus is resident.

For recovery from the trigger effect (overwriting the MBS), a generic boot protection program installed before infection, which maintains a copy of the relevant boot sectors on floppy disk, would make recovery virtually instantaneous.

Conclusions

Despite all the effort which has gone into production, it is possible (even probable) that Barrotes' arrival on a system would cause only the slightest pause in normal computing. Although the symptoms of the trigger routine appear serious, it is not difficult to recover the data from the disk.

It is likely that a small outbreak of this virus would not be thought worth reporting to the Police, but I would ask *all* users to report virus attacks: this is the only way in which we stand any chance of maintaining an accurate picture of the virus problem and bringing the perpetrators to book.

Barrotes

Aliases:	None known.
Type:	Resident, Appending, Parasitic.
Infection:	EXE files and COM files between 254 and 64000 bytes long.
Self-recognition in Files:	Value 534Fh (ASCII 'SO') located at either the end of file or at offset 816 from the file end.
Self-recognition in Memory:	'Are you there?' call made by inserting EEh into AH, call Int 21h. Return value is FEh in AL.

Hex Pattern:	In memory and in infected files.
	`0510 002E 0144 732E 8E54 7333`
	`C02E 8344 3910 2EFF 6C37 534F`

Intercepts:	Int 21h subfunction EEh for 'Are you there?' call. Int 21h subfunction 4B00h for infection of target file.
Trigger:	If virus becomes resident on 5th January, displays message and coloured bars across the screen. Overwrites MBS of first fixed drive.
Removal:	Complete specific disinfection possible under clean system conditions. Reboot from clean system floppy, then identify and replace all infected files. Data recovery after the trigger is possible.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

VIRUS ANALYSIS 2

AVV - The Anti-Virus Virus

Eugene Kaspersky

Of the thousands of computer viruses now known, many have no function but replication. There are, however, a few viruses which have a particularly damaging trigger. These may erase data on fixed disks, corrupt programs, erase the contents of CMOS memory, or hang the system. Such viruses tend to be well known - two examples are Michelangelo and Disk Killer.

A step down from these blatantly malicious samples are those with a supposedly humorous trigger. Many viruses display a message or produce a sound effect: for example, Form causes the PC speaker to produce a click when a key is pressed, Tequila displays a multi-coloured Mandelbrot set, HH&HH launches a round ball which bounces on the screen, and Playgame starts a computer game - this is probably highly amusing for the virus writer, but an annoying nuisance for the user.

At the bottom of the damage scale are viruses with 'semi-beneficial' trigger routines, such as Yankee Doodle, which announces, 'it's the end of worktime, let's go home', accompanied by a tune. The Kiev virus also attempts to be useful, by helping the user keep track of the time by beeping six times on the hour, every hour. However, the most potentially useful trigger of any virus so far is Cruncher (*VB*, June 1993, pp.8-9), which can actually save disk space on infected machines by compressing infected files.

What more can a virus do to an infected system? It seems like the only limit to the possibilities for trigger routines is the imagination of the virus author. Perhaps the most unusual payload of any virus is one which identifies and destroys any other viruses it encounters: an anti-virus virus!

A Brief History

Although anti-virus viruses are a relatively new phenomenon, there are already a handful of viruses known to attack infected programs. The first example I discovered was Pentagon. When this virus infects a diskette, it checks for the presence of Brain: if found, Pentagon removes the Brain virus from the disk before infecting it with itself.

A second such example is Yankee Doodle (version 44). When a file infected with this virus is executed, the system memory is checked for the presence of the Italian virus. If it is detected, the memory-resident component of Italian is altered so that further infections of the virus will only replicate through 255 generations. Shortly after distribution of this version of Yankee Doodle, further anti-virus capabilities were added to it: version 46 can disable the memory-resident code used by Cascade.

These are two examples of 'good' trigger routines, but they are a far cry from being efficient or dependable, and do not exonerate the virus writer's actions. In each case, the viruses make unauthorised modifications to code stored on the host machine, and are capable of dealing with only one or two viruses - far below the standard of good anti-virus software. Now, however, the first virus with 'ready to use' anti-virus capabilities has appeared: AVV, the anti-virus virus.

Overview

AVV is a 2300-byte non-memory-resident virus infecting only COM files. It functions by searching for other COM files in the same directory and, when it finds them, prepends its own code, just like the Jerusalem virus.

> *"The most unusual payload of any virus is one which identifies and destroys any others it encounters: an anti-virus virus"*

AVV infects only files between 2500 and 60000 bytes long. When a suitable file is found, its attributes, time, and date stamp are stored and cleared before infection. These are reset once the file has been infected. During this process, the virus hooks Int 24h (the DOS Critical Error Handler), thus preventing the display of any error messages produced.

Before infecting host files, AVV ensures that it has unrestricted access to the DOS Int 21h handler. The original Int 21h vector is obtained, using a tracing procedure copied from the Yankee Doodle virus. When this is complete, the virus hooks Int 2Ah and replaces the original handler with an IRET instruction. This will disable certain anti-virus monitors, but can also cause *NetWare* to crash when running on a non-dedicated file server.

Anti-viral Features

The general aims of AVV can be seen by examining the following text strings contained within the virus:

```
The AVV version 1.12, Copyright (C) 1992 n (ARV)
AVV Warning! In file filename.ext may be virus.
AVV Warning! In system area may be virus.
AVV Warning! In system may be virus. AVV=off
The AntiVirus Virus version 1.12 AVV112: I am check
200++ viruses
Thank's Yankee Doodle for original vectors
(ARV)
```

Finally, AVV checks the system's DOS environment: if the string 'AVV=off' is found, the virus disinfects the host file when it is executed. This gives the user a straightforward method of cleaning up a single infected file. Simply typing

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

the command 'SET AVV=off' at the DOS prompt, and executing the infected file will cause the virus to remove itself automatically from that file.

When an AVV-infected file is executed, the virus attempts to check that the system contains no other viruses. Several different methods of detection (both specific and generic) are used, each of which is listed below.

When AVV receives control, it first checks the contents of the SI register. If this is not equal to 0100h, the virus displays the warning message:

```
AVV Warning! In system may be virus.
```

This method of virus detection relies on an undocumented feature of DOS. When a COM file is loaded into memory, DOS loads the SI register with the value 0100h. If the AVV-infected file subsequently becomes infected by another virus which does not explicitly reset this register, the contents of the SI register will probably have been changed. Therefore, if SI is not equal to 0100h, it is reasonable to assume that the file has been infected. Many viruses, including most Vienna variants, can be detected by this simple test.

Viruses may also be detected through examination of the first instruction of the original Int 21h handler - the virus will calculate the address via the tracing routine. If that first instruction is a JMP FAR (opcode EAh) which does not point into upper memory, the virus displays the message:

```
AVV Warning! In system area may be virus.
```

This routine is designed to detect viruses which overwrite the first instruction of the original DOS Int 21h handler with a far jump to themselves. The jumps to high memory are excluded because DOS 5.0 and 6.0 use this construction to load the body of its code into high memory. This method of redirecting calls to the DOS handler is used by several of the more complex stealth viruses.

Infection and Detection

When these generic virus detection tests are completed, the virus searches for other COM files in the same directory, reading several bytes at the start and end of each file into memory. This is done for the dual purposes of infection and virus detection. Checks for the presence of other viruses are done by carrying an elementary hex pattern search on the target file. For example, AVV checks the beginning of the file for the text string 'sURIV' (as found in COM files infected with April 1st). It also searches files for the 'MsDos' text string, or for part of its code, with which it can identify some versions of Jerusalem. Through such elementary methods, AVV is capable of detecting a number of viruses and virus families. Where this happens, AVV displays the message:

```
AVV Warning! In file FILENAME.EXT may be virus.
```

where FILENAME.EXT is the name of the infected file.

If no viruses are found, AVV checks the file date/time stamp. When an incorrect value is displayed (eg. 62nd day), AVV displays a warning message. I do not know exactly how many viruses AVV detects, but the copyright string states: 'AVV112: I am check 200++ viruses'. Two hundred-plus viruses detected by just one other - not a bad result.

If a file is not infected, and the time and date are correct, AVV will infect it. However, no warning message is displayed if the file concerned is already infected by AVV. This shows bias on the part of the author. For example, if an AVV-infected file is run when infected by 4K, a fully stealth virus, AVV will display the following messages:

```
AVV Warning! In system may be virus.
AVV Warning! In system area may be virus.
AVV Warning! In file FRODO.COM may be virus.
```

Possible Consequences

AVV is the second virus I have encountered with a trigger routine which could be considered beneficial (Cruncher was the first). It is hence possible to find things other than destructive triggers in viruses: in these two, run-time compression of executable files and anti-virus scanners.

What will come next? A *Windows* virus which includes a word processor? [*Please insert Windows virus disk 5 and press return… Ed.*]. What is the borderline between a useful program and a virus? It is easy to make DOS self-replicate. Does this mean that DOS is a virus? The difference which makes one program a virus while another is not seems to be one of intent and motivation. AVV is definitely a virus, but as time progresses, I find it harder and harder to decide where to draw the line.

Anti-Virus Virus

Aliases:	None known.
Type:	Non memory-resident, parasitic.
Infection:	COM files only.
Self-recognition in Files:	Checks ID-word 'AV' in file beginning at the offset 8.
Self-recognition in Memory:	None.
Hex Pattern:	`B9FF FFF2 AE26 3825 75F6 83C7` `03B8 023D 8BD7 061F E8C1 FE0E`
Intercepts:	Int 24h to disable DOS write-protect error messages and Int 2Ah to disable antiviral monitors.
Trigger:	Displays warning messages (see text).
Removal:	Under clean system conditions, either identify and replace infected files or type 'SET AVV=off' from DOS prompt and run an infected file.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

VIRUS ANALYSIS 3

Riotous Assembly

James Beckett

When people involved in the fight against viruses complain that the phenomena are predominantly rather dull, it is most certainly not an invitation to the authors to try harder. Now, however, another 'wish' has been fulfilled, in the emergence of a more advanced virus - Cyber Riot, the first which is capable of infecting the *Windows* Kernel.

Knowledge of *Windows'* internals is clearly becoming more widespread - Cyber Riot uses several *Windows* functions not documented in any of the Developers' Kits. Virus writers have once again found the knowledge they require, whether from published books such as Pietrek's *Windows Internals* and Shulman's *Undocumented Windows*, or through reverse-engineering *Windows* code. The fact that such information is not available from *Microsoft's* documentation makes the entire disassembly process doubly painful.

Previous *Windows* viruses have operated fairly simply - WinVir_14 was a non-resident one-shot virus, whilst Twitch searched systematically through the disk for targets. In DOS, these methods of infection have met with only limited success, so most DOS viruses intercept file or disk accesses to infect files 'on demand'. Cyber Riot is the first *Windows*-specific virus to remain resident and to intercept the execute function by infecting KRNL386.EXE - this is equivalent to infecting the DOS hidden system files (eg. IO.SYS etc.).

Windows System Files

The *Windows* system is based largely on special EXE files kept in the SYSTEM directory - KRNL386.EXE, USER.EXE, and GDI.EXE. Functions called by *Windows* applications are dynamically linked to these files at run time: for example, GDI.EXE contains functions for the Graphical Device Interface (basic line drawing, window operations, clipping, palettes and so on). USER has higher-level functions for Dialog boxes, Cursors, Icons, etc. The KERNEL module (from KRNL286.EXE or KRNL386.EXE) provides for fundamentals like task switching, memory allocation and event handling. All these functions combine to make the *Windows* 'set-up'.

One particular function of the Kernel module KRNL386.EXE, WinExec, is used for starting up new applications. This is typically called by Program Manager or File Manager when an icon or name is double-clicked, or when the Run command in the File menu is used. In DOS, viruses normally intercept Int 21h, subfunction 4B00h (the DOS Load_and_Execute command). The comparable *Windows* function is WinExec: this cannot be intercepted by an active application. Therefore, the authors have had to find an alternative method of subverting it.

Infection Procedure

When an application infected with Cyber Riot is run, the virus searches for the file from which the KERNEL module came, using the *Windows* function designed for that purpose. It opens the file, checks that it is a segmented executable and not already infected, by looking for a checksum value which corresponds to the text 'LROY' (the virus' infection marker). Before proceeding, it attempts to back the file up by changing the EXE extension to EXF.

Infecting *Windows* executables is a complex task - a subset of operations performed by the link stage in a program compilation. This is more difficult than the simple appending one can do to a DOS COM file and the minimal fixup required to a DOS EXE file. All the dynamic-linking which makes up the *Windows* API requires that a vast amount of information be held in the header of a program file, in order to control how it loads. When infecting a file, this must be analysed, copied and modified so that the resulting file still works as intended, albeit with the new virus code attached.

"On return from the MessageBox function the virus starts on a wave of destruction through the fixed disks"

Some 800 lines of code have been written to this end, enabling infection of both standard executables and the kernel file, which is structured in a different manner to other *Windows* files and needs a different strategy. The basic operation is to add an entry to the segment table (roughly speaking, the table of contents for the file) for its own single 3272-byte segment, then adjust the rest of the file to accommodate itself.

Functions which can be called from other programs must be declared so that *Windows* executables can link to them - this is done by entries in the header. The virus patches this information so that the WinExec function points to its own code. The address of the original entry point is kept, so the virus can call it. When this process is complete, the virus immediately jumps back to start the host application as if nothing had happened. This is new in comparison with older *Windows* viruses, which were not capable of passing control back to the host file - it was necessary to issue the execute command a second time. It is this property which represents a significant advance on the part of the virus authors.

Nothing more happens until *Windows* is exited and restarted - modifications have been made to the file on disk, but not loaded into memory. Once loaded, the new kernel module uses the virus code to subvert the WinExec function.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

MessageBox

When a new program is executed, the ersatz WinExec first calls the original *Windows* handler, so that the program starts immediately. The virus then considers the file for infection, just as it did the Kernel file. However, after infection, a trigger routine may activate. The virus has already made a dynamic link to a USER module function for displaying a message box, and now checks the date. On certain dates, it displays a message in a window using the MessageBox function. All bear the title:

```
Chicago 7: Cyber riot
```

A different message is printed in the box according to the date of the trigger - from April 29th to May 1st:

```
Happy anniversary, Los Angeles
Anarchists of the world, unite!
```

On any Friday before the 13th of a month:

```
When the levee breaks, I have no place to stay...
(Crying won't help you. Praying won't do you
no good)
```

And on any Saturday in March 1994:

```
Save the whale, harpoon a fat cat.
```

Harmless enough, perhaps, but pressing OK might not be a good idea: on return from the MessageBox function the virus starts on a wave of destruction through the fixed disks, writing part of the virus code over the first sector of each of tracks 1 to 255, heads 0 and 1. It omits the Master Boot Sector and DOS Boot Sector, but many files will be at least partly corrupted - one sector of corruption can be disastrous. One wonders why the authors conscientiously back up each infected program when such a routine is incorporated.

Chicago 7

The virus contains a number of text messages scattered throughout the code. They are not encrypted, nor has any attempt been made to hide them. Some are the text for the messages mentioned above, but several are never printed.

The first of these seems to make a rather contradictory claim of the date of writing, mentioning both January 1993 and summer of the same year. Another hints at more to come in the same line, with an askance poke at the soft drink industry's advertising: 'Coming soon: Diet Riot. Same great aftertaste, fewer bytes.' If this really is targeted at compression algorithms, anti-virus software companies will have to think carefully about their compressed-file scanning.

Yet another message offers the source code, for $15,000,000, but probably nobody will take advantage of the authors' kind offer. The file position of another suggests it might have been meant as part of the second MessageBox, though the text, 'Convict the pigs', is unrelated. There is also a complaint, which could be a genuine grouch, or a red herring: 'Why does *IBM* need to lay me off? Oh well, their loss.'

Finally, a cryptic comment, accusing anti-virus product vendors of making money out of hype and user confusion: 'McAfee's FUD equation: !!!!!!+?????? = $$$$$$'.

Whether copyright infringement could become an issue with regard to virus disassembly by researchers has yet to be seen, but many viruses contain messages claiming ownership. In this case, there is almost a biography: 'This program was written in the cities of Hamburg, Chicago, Seattle and Berkeley. Copyright (C) 1993 Klash/Skism/George J/ Phalcon/Henry Buscombe and 2 ex-Softies, collectively known as the Chicago 7'.

Skism and Phalcon are well-known names, creators of PS-MPC (Phalcon/Skism Mass-Produced Code generator), but Chicago 7 seems to be a new alliance, promising many amusing days to come.

Summary

As part of the kernel, the virus is not readily detectable in memory, but a checksummer should detect the changes made to the infected files. In order to be precise about detection specifications, the structure of the executable file and ways of tracking down entry points need discussion, but this would require much greater depth than time and space allow here. Simple patterns suffice for a basic scanner, but any sensible system would locate the area required in the file before accepting this string as significant.

Cyber Riot is limited to *Windows* systems and cannot, as such, propagate under DOS. Unfortunately, this does not mean that spread of the virus will be restricted, as many people now use only *Windows*, finding a DOS command-line interface problematic. The virus may yet get somewhere, if people do not notice the extra time the hourglass is on their screen. As with all viruses, it is essential to check out any anomalies in your operating system; only thus is it possible to limit their propagation.

Cyber Riot

Aliases:	None known.
Type:	Parasitic file infector.
Infection:	*Windows* Kernel programs.
Self-recognition in Files:	String 'LROY' in EXE checksum.
Self-recognition in Memory:	Not applicable.
Hex Pattern:	offset 013Ah from end of start segment.

```
B40D CD21 0E07 8B5E F8B9 8000
518A D1B9 FF00 518A E9B8 0302
```

Intercepts:	*Windows* Kernel WinExec function.
Trigger:	Displays message on various dates.
Removal:	Delete infected EXE files, and rename corresponding EXF to EXE. Reload KRNL.EXE files from *Windows* disk.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

COMPARATIVE REVIEW

1994 Scanner Test

Mark Hamilton

The *Virus Bulletin* comparative scanner test has now established itself as a traditional January event, and provides readers with an excellent insight into the efficacy of their chosen product. This year the field has reduced very slightly, with only nineteen different products actually making it to the starting blocks.

The most important attributes measured in this review are:

- The ability to detect viruses known to be in the wild.
- The ability to keep up to date with a rapidly increasing number of viruses.
- The speed of the scanner.

All developers and vendors were invited to submit copies of their latest version for testing. The turnout was excellent, with only a handful of absentees. Products unavailable for testing because they have been discontinued over the last year include *NOVI*, *Untouchable*, and *Xtree Allsafe*.

The 'In the Wild' and 'Standard' test-sets have been modestly expanded to include viruses which have either become common or are particularly difficult to detect. Full details of the test-sets are given at the end of the review.

All the products were tested on a *Compaq* 386 running at 16MHz. The hard disk speed test used the *Compaq's* 42 Mbyte drive which was compressed using *Stacker* to provide 113 Mbytes of theoretical disk storage capacity. The drive actually contained 45,818,823 bytes in 1,769 files, of which 19,414,441 bytes (375 files) were executable. The floppy disk speed test measured the time to scan a 3.5-inch high density diskette which contained 43 files (1,446,811 bytes), all of which were executable.

AVScan Version 1.25

In the Wild:	100%
Standard:	99.7%
MtE:	100%
Verdict:	Excellent for a freeware product.

AVScan is a 'freeware' scanner distributed by *H+BEDV*, and can be downloaded from a number of bulletin boards including the Virus Forum on *CompuServe*. The scanner acts as advertising material for the company's much more complete anti-virus package *AntiVir IV*, which, unlike *AVScan*, is only available in German. The product ranks well above many of its 'payware' rivals, missing only one virus.

Central Point AntiVirus Version 2.1

In the Wild:	91.5%
Standard:	97.3%
MtE:	Failed to complete test.
Verdict:	Mediocre.

Among the eight viruses missed from the In the Wild test-set were Powerpump and Todor. However, *CPAV's* identification of the boot sector viruses included in the test-set left something to be desired: both the Quox and Monkey viruses were detected simply as 'Viral Code B'.

One of the confusing and unexplained mysteries surrounding this product is that, unless *CPAV* is configured to allow network access, the user cannot scan any external drives or devices. This needs to be made clear in the manual.

A couple of other problems were discovered during testing. The product ran very slowly when scanning infected drives, taking over 40 minutes to scan the drive holding the Standard test-set. In addition, *Central Point* does not appear to have sorted the problem reported in last year's comparative review: the product *still* unceremoniously crashes and hangs the PC when more than 255 infected files are found.

In terms of speed and detection, *CPAV* now lies towards the back of the field. Overall, a disappointing result.

Microsoft AntiVirus

In the Wild:	75.5%
Standard:	94.1%
MtE:	Failed to complete test.
Verdict:	A useful prophylactic, but inaccurate.

Although *Microsoft* has released a new version of *MS-DOS* which contains a more up to date version of its scanner, the company chose to submit *MS-DOS 6.0* for this review.

MSAV missed viruses from both the In the Wild and the Standard test-sets. Some of the viruses it failed to detect have been in circulation for many months. *MSAV* also failed to complete the MtE test - each time it ran, it caused the Memory Manager (also a *Microsoft* product) to terminate the DOS session with an Exception Error. Not an auspicious result for two products supposedly from the same stable.

The fact that it is a reasonably fast scanner will come as cold comfort to those who rely on it. *MSAV* can detect most common viruses, and as such, it is a useful addition to DOS. However, it would be difficult to advise its use on systems where virus prevention is a must rather than a luxury.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

Package	In the Wild File Infectors (80)	In the Wild Boot Sectors (14)	Standard (371)	Mutation Engine (1926)	Overall Accuracy (100)
AVScan	80	14	370	1926	99.9
CPAV	72	14	361	Failed to Complete	83.6
Dr Solomon's AVTK	80	14	371	1926	100
F-Prot	80	14	371	1926	100
IBM AntiVirus	80	14	371	1926	100
Iris AntiVirus+	68	13	362	1926	89.8
McAfee SCAN	77	14	364	1926	97.4
MSAV	59	12	349	Failed to Complete	71.7
Norton AntiVirus	75	12	367	1926	94.6
PC-cillin	62	12	361	0	74.6
PCVP	74	13	366	1926	94.5
Sophos' Sweep	80	14	371	1926	100
TB Anti-Virus	80	14	371	1926	100
The Doctor	70	13	359	1926	91.2
VET	77	14	360	1817	96.6
Virus Buster	Failed to Complete	Failed to Complete	Failed to Complete	Failed to Complete	N/A
VirusCure Plus	68	14	360	1926	90.5
VIS	66	13	367	1926	88.6
Vi-Spy	80	14	371	1926	100

Food for thought: This year, six products achieved perfect scores in all the tests. These were *Dr Solomon's Anti-Virus Toolkit, F-Prot, IBM AntiVirus, Sophos' Sweep, ThunderBYTE Anti-Virus* and *Vi-Spy*. The overall score of each product has been calculated by weighting the performance against each test-set as follows: In the Wild, 70, Standard, 20, Mutation Engine, 10.

IBM AntiVirus Version 1.04

In the Wild: 100%
Standard: 100%
MtE: 100%
Verdict: An excellent addition to *PC-DOS*.

This is the fourth release of *IBM AntiVirus* since *IBM* completely rewrote and re-released the product in November 1992. Although upgrades to the product are only released quarterly, it nevertheless manages to keep up to date. It found all the samples in the *Virus Bulletin* test-sets without any problems whatsoever - a creditable performance.

Rather than simply scanning the disk every time the product is run, *IBM AntiVirus* maintains a checksum database of all files on the disk, and scans only those files which have changed. This means that the product is slow to scan a disk for the first time, but much faster on subsequent scans.

I still find its user interface somewhat quirky and it takes some time to become accustomed to its *modus operandi*. For example, it is extremely difficult to select all the program files on just one hard drive or partition. I found I had to add each directory to be checked in turn, a procedure which was unwieldy and time-consuming.

IBM AntiVirus for both *DOS* and *Windows* is bundled as part of *IBM PC-DOS 6.1* and as such, represents tremendous value for money. A class above *MSAV*.

PCVP Version 1.23

In the Wild: 92.6%
Standard: 98.6%
MtE: 100%
Verdict: Fairly fast but lacks detective powers.

PCVP scan speed is quite impressive (over 300Kbytes per second), but is let down slightly by its detection results. It missed Power Pump, SBC, WinVir_14, Butterfly, Satan Bug and Quox, in the In the Wild test-set. The program includes a mouse and menu-driven front end, though it can also be command line driven, making it suitable for inclusion in batch files.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

Package	Hard Drive Scan (minutes and seconds)	Hard Drive Scan (Kbytes per second)	Floppy Disk Scan (minutes and seconds)	Floppy Disk Scan (Kbytes per second)
AVScan	2:29	127.0	1:23	17.0
CPAV	4:01	78.7	2:20	10.1
Dr Solomon's AVTK	1:12	263.3	0:37	38.2
F-Prot	1:45	180.6	0:37	38.2
IBM AntiVirus	1:42	185.2	1:58	12.0
Iris AntiVirus+	1:33	203.9	0:57	24.8
McAfee SCAN	5:50	54.2	2:50	8.3
MSAV	3:37	87.2	1:12	19.6
Norton AntiVirus	0:54	351.1	0:25	56.5
PC-cillin	1:39	192.5	1:27	16.2
PCVP	1:02	303.4	0:47	30.4
Sophos Sweep	7:56	39.9	3:38	6.5
TB Anti-Virus	0:38	498.9	0:17	83.1
The Doctor	4:00	79.1	1:28	16.0
VET	0:56	339.2	0:35	41.0
Virus Buster	Failed to Complete	Failed to Complete	Failed to Complete	Failed to Complete
VirusCure Plus	9:31	33.2	3:01	7.8
VIS	10:05	31.3	4:34	5.2
Vi-Spy	1:58	161.0	1:37	14.5

You want it when!? Scan speeds varied wildly during this test, ranging from an unbelievable 38 seconds to a whopping time of over ten minutes. It is interesting to note that, of the six scanners which achieved perfect scores, nearly all have above average scan speeds, showing that it is possible to have one's cake and eat it! It should be noted that many of the scanners slow down drastically when scanning an infected disk.

Iris AntiVirus+ Version 4.20.22

In the Wild: 86.2%
Standard: 97.6%
MtE: 100%
Verdict: Considerable room for improvement.

Iris gets an immediate black mark for supplying its product on write-enabled floppy disks. *AntiVirus+* is not quite as good as its manual or accompanying advertising literature would have you believe. Among the common viruses it failed to detect were Father, Hidenowt, Necros, Satan Bug, Starship and Quox. All these viruses are known to be in the wild - *Iris* needs to improve these scores drastically. Although it found all MtE infections, it missed several viruses in the Standard test-set.

AntiVirus+ is not one of the fastest packages, but neither is it unusably slow - it ran at a respectable 204 Kbytes per second during tests.

Overall, *AntiVirus+* needs to improve its detection capabilities considerably before I am prepared to recommend its use.

McAfee SCAN Version 9.29 V108

In the Wild: 92.6%
Standard: 98.1%
MtE: 100%
Verdict: In danger of becoming outdated.

Sporty DOS and *Windows* front-end programs are now provided as standard with *SCAN*, the best-known of the US-produced packages. However this merely seems to be window-dressing to try and vitalise a flagging product.

The scanner failed to detect the Loren and Power Pump infections from the In the Wild test-set, as well as some of the older viruses from the Standard test-set. SCAN was once one of the faster products available - now it is one of the slower ones.

Its availability as shareware - which to many means without cost - guarantees its continuing survival. However, users who are serious about detecting viruses should now start to consider other alternatives, even though this almost inevitably means paying more for peace of mind.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

Dr Solomon's Anti-Virus Toolkit Version 6.56

In the Wild: 100%
Standard: 100%
MtE: 100%
Verdict: Trusted and effective.

There is very little one can say about this product. It is consistently good, and has deservedly become one of the benchmarks by which other anti-virus products are measured. It is not, however, the fastest *and* most accurate product - this position has now been usurped by *ThunderBYTE Anti-Virus* from *ESaSS*.

F-Prot Version 2.09F

In the Wild: 100%
Standard: 100%
MtE: 100%
Verdict: Excellent performance.

Frisk Software has a reputation for producing a high quality virus scanner, and this version is no exception. It achieved a perfect score against all the test-sets, although it does seem to be getting slower in operation.

F-Prot is an excellent scanner for any anti-virus tool-chest. In the UK, it is marketed and supported by *Reflex Magnetics*, though the latest versions continue to be available from *CIX* and *CompuServe* - as well as by anonymous ftp from several Internet sites. A non-shareware version of the product is now available, boasting enhanced heuristic detection and additional features. Recommended.

Norton AntiVirus Version 3.0

In the Wild: 92.6%
Standard: 98.9%
MtE: 100%
Verdict: Much improved, but still needs work.

Like so many other scanning products, *Norton AntiVirus* is let down by its inability to detect certain viruses - the reason one buys a scanner in the first place. Nevertheless, the user interface, manuals and assorted trimmings are all of a very high standard, and the product is fast and easy to use.

The product's virus detection rating has increased since last year, but not enough for it to gain perfect scores. *NAV* missed seven viruses known to be in the wild. This may be a problem with the age of the product, as the file date of the scanner was 20th September 1993. *NAV 3.0* shows promise, and may well improve over the coming year.

PC-cillin Version 3.65

In the Wild: 78.7%
Standard: 97.3%
MtE: 0%
Verdict: Not recommended.

This product was fully reviewed by Dr Keith Jackson in last month's edition of *Virus Bulletin*. It is the least accurate of all the scanners tested. This is due partly to its age and partly to the fact that it is incapable of detecting polymorphic viruses. This product has no redeeming features, and as an added 'bonus' requires the use of a dongle.

Sophos' Sweep Version 2.55

In the Wild: 100%
Standard: 100%
MtE: 100%
Verdict: Stable and reliable.

Sweep has changed little over the years, and has earned a reputation for being reliable and effective. The most noticeable improvement to the product is the addition of SW, a CUI-compliant DOS front end. While not a particularly fast product (though the product runs several times faster in its 'quick' mode), it is always in the top handful of products in comparative reviews. Very reliable.

ThunderBYTE AntiVirus Version 6.08

In the Wild: 100%
Standard: 100%
MtE: 100%
Verdict: Blinding speed and accuracy.

TBAV is a product which has improved dramatically over the years. Not only has it become faster and more accurate, but the user interface has improved as well. All the various components can now be called from the central menu program, *TBAV*, or directly from the command line, allowing for flexibility of operation.

As well as an excellent scanner, the user can add his own hexadecimal search strings to the product. This is complemented by the facility to carry out an optional scan of the files using heuristics. The heuristic portion of earlier versions was prone to mistakes, identifying innocent programs as being infected: this version made no such errors.

The product scored perfect results against all the test-sets used, as well as earning the honour of being the fastest scanner. This is a very impressive result, and *TBAV* deserves to be seriously considered as a useful and active part of any anti-virus toolkit.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

VirusCure Plus Version 3.12 V102

In the Wild: 83.0%
Standard: 97.0%
MtE: 100%
Verdict: Pretty interface, lacklustre performance.

VirusCure Plus is a hotch-potch of programs developed by *IMSI* using *McAfee Associates'* scanner technology. Its manual is appallingly brief and does not explain many of the scanner options.

Unfortunately, the on-line help is of little more assistance: for example, pressing F1 with the Scanner Options dialogue box open results in a help page, which briefly describes what the program means by scanning: hardly what the user wants. *IMSI* would be well advised to improve this.

Among the viruses *VirusCure Plus* missed were Tremor, Starship, Hidenowt, Coffeeshop, Butterfly and Satan Bug, from the In the Wild test-set. It also missed the newer additions to the Standard test-set, as well as some old favourites like Casper. It was only just faster than *VIS*, the slowest of all products tested.

The Doctor Version 3.98

In the Wild: 88.3%
Standard: 96.8%
MtE: 100%
Verdict: Possible danger of false positives.

The Doctor is a new product from *Thompson Network Software*, based on *Leprechaun's Virus Buste*r.

Whilst scanning a known clean hard drive - for the speed tests - *The Doctor* identified two perfectly innocent files as infected: one in the shareware archiver ARJ.EXE and the other in the TSR management utility MARK.COM, a fact which I find rather disconcerting.

It missed the EXE version of Invader, both versions of Loren, Necros, Powerpump, Sibel Sheep, Starship and WinVir in the In the Wild test-set: a disappointing result. The Standard test-set results continued in the same vein, where, in addition to missing all the more recent additions, it also missed some of the older viruses.

The software is afflicted with bugs, one of which seems to prevent it from running in batch mode. This means that every time it discovers a virus, the user is presented with a menu of options for proceeding. This might not pose a problem for most users, but for product testing it most certainly does - particularly when using the MtE test set! It is very early days for *The Doctor*, and although these results are not awe-inspiring, it is to be hoped that the developers will significantly improve the detection figures.

Virus Buster Version 4.01

In the Wild: Failed to complete tests.
Standard: Failed to complete tests.
MtE: Failed to complete tests.
Verdict: Difficult to tell.

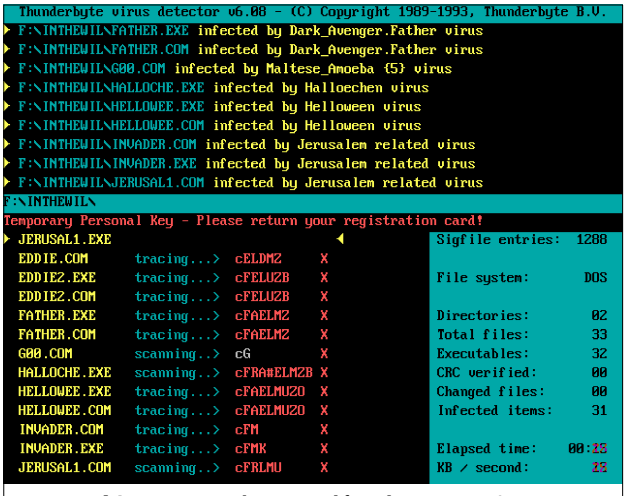
The product installed correctly, but all attempts at running the scanner (BUSTER.EXE) were thwarted. The test PC hung on every occasion with the simple message 'Internal stack overflow, System halted'. I seem to recall an earlier version of the program which presented me with a similar problem in the last comparative review. *Leprechaun* had also included a new scanner, called *V-Mini*. Unfortunately, this too failed to work, and terminated with a runtime error message. The only part of the package successfully tested was a *VBuster* ballpoint pen. This functioned well, though as a word processor, it was prone to making mistakes.

VIS Anti Virus Utilities Version 4.2

In the Wild 84.0%
Standard 98.9%
MtE 100%
Verdict: Disappointing.

Total Control supplies a DOS CUI, *Windows* GUI, and DOS command line versions of its programs. The company has beautified the *Windows* interface by the simple expedient of adding *Borland's* custom controls, but this does nothing for the efficacy of the product.

Apart from being the slowest product tested, its detection rate is also too low. Among the file-infecting viruses it missed in the In the Wild test-set were Coffee Shop, Loren, Necros, Powerpump and Tremor. Its detection of boot sector



Fast and Accurate. Much improved from last year, *TBAV* seems to be going from strength to strength. Will *TBAV* retain this position in the next *VB* comparative review?

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

viruses was better, where it missed only the Quox virus. *VIS* did find all the MtE samples, but at some cost - it took over 3 hours to complete its scan of the 1,926 samples.

Before *VIS* became the good-looking, mouse-driven program it is today, it was fast, deadly accurate and reliable. Somewhere during the last two years the product has lost its way, and now has little to recommend it.

VET Version E7.4

In the Wild:	92.6%
Standard:	97.0%
MtE:	94.3%
Verdict:	MtE detection needs improving.

VET failed to detect Starship, Satanbug and WinVir_14 from the In the Wild test-set. It also missed some of the older viruses in the Standard test-set, most notably Machosoft and Diamond A. *Cybec's* MtE detection algorithm requires some attention - *VET* has the dubious honour of being the only product to detect some samples, rather than the 'all or nothing' results of its competitors.

VET is a command line driven product, and does not have any fancy front-end software to slow it down. Well-known 'down under', the product needs to improve its virus detection in order to distinguish itself from the competition.

Vi-Spy Version 11.0 Rel.09.93

In the Wild:	100%
Standard:	100%
MtE:	100%
Verdict:	Efficient, accurate and reliable.

Vi-Spy is head and shoulders above most other American anti-virus products, both in terms of overall design and accuracy. The scanner takes a no-frills approach, and combines speed with reliability. This, coupled with the good performance of the TSR component of the product (see *VB*, September 1993, pp.18-19), makes *Vi-Spy* a strong competitor to other, better-known names.

Observations

The most telling results in this review were not from the top-scoring products, but from those which failed the various tests. It can be clearly seen that certain vendors products are beginning to flag under the volume of new viruses.

The purpose of the *Virus Bulletin* comparative reviews is not to tell users which product to buy - rather it should show which products *not* to buy. Readers should examine these results with care - if their product failed, they have every right to ask the developer why.

The Test-sets

1. In the Wild

Where appropriate, one genuine COM and one EXE file infection of: 1575, 2100, 4K, 777, AntiCAD, BFD-351, Butterfly, Captain Trips, Cascade 1701, Cascade 1704, Coffee Shop, Dark Avenger, Dark Avenger, Dir II, Eddie 2, Father, Flip (20 COM and 20 EXE), Hallochen, Hide Nowt, Jerusalem, Keypress, Maltese Amoeba, Mystic, Nomenklatura, Nothing, PcVrsDs, Penza, Satan Bug, SBC, Sibel Sheep, Slow, Spanish Telecom 1 (5 COM), Spanish Telecom 2 (4 COM), Spanz, Starship, 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, Monkey, New Zealand 2, NoInt, Quox, Spanish Telecom, Tequila.

2. Mutation Engine

This test-set consists of 1,926 genuine infections of the Groove virus, which uses Mutation Engine encryption.

3. Standard

Where appropriate, one genuine COM and one EXE file infection of:1067, 1077, 1226, 1260, 2480, 3445, 440, 4K, 5120, 555, 789, 800, 8888, 8 Tunes, Advent, Agiplan, Aids, Aids II, Akuku, Alabama, Ambulance, Amoeba, Amstrad, Amstrad Cancer variant, Anthrax, AP-605, AP-529, AP-480, AP-440, AP-400, Armagedon, Attention, Bebe, Best Wishes 1, Best Wishes 2, Blood, Black Monday, Bulgarian 1600, Bulgarian 1600 v2, Bulgarian 1600 v21, Bulgarian 492, Bulgarian 905, Burger 1, Burger 2, Burger 3, Burger-405, Carioca, Cascade Family (01, 04, Y4), Format, Casino, Casper, Christmas in Japan, Christmas Tree, Christmas Violator, Cookie, Crazy Eddie, Dark Avenger, Dark Avenger-2100, Dark Avenger 3, Datacrime Family (1, 2, II, IIB), Datalock, Dbase, DBF Blank, December 24, Deicide, Destructor, Devil's Dance, Diamond A, Diamond B, Dir, Diskjeb, Do Nothing, Do Nothing 2, Doom 2, Dot Killer, Durban, Dyslexia, Eddie-2, Evil, Faust, Fellowship, Fichv, Fish.1100, Fish-6, Flash, Flip, Fu Manchu, Gergana, Ghostballs, Guppy, Halley, Hallochen, Hybrid, Hymn, Icelandic 1, Icelandic 2, Icelandic 3, Int 13, Internal, Invisible, Iraqi Warrior, Itavir, Jerusalem Family (4th Black Friday, A204, Anarkia, AntiScan, B, C, GP1, Groen Links), Kylie, Mendoza, PLO, PSQR, USA, Westwood, Jocker, Jo-Jo, Joker-01, July 13th, Justice, Kamikaze, Kemerovo, Kennedy, Keypress, Lehigh, Leprosy, Leprosy B, Liberty 1, Lovechild, Lozinsky, Machosoft, MG, MG-1, MG-2, MG-3, MG-4, MGTU, Micro-128, Minimal-45, Mirror, Mix1, Mix1-2, Mix2, MLTI, Monxla, Murphy-1, Murphy-2, Nina, Nomenklatura, NTKC, Nukehard, Number of the Beast Family A, B, C, D, E, F, Number 1, Old Yankee 1, Old Yankee 2, Ontario, Oropax, Parity, PcVrsDs, Perfume, Phantom, Phoenix, Pixel Family (1, 2, 3, 5), Plastique Family (AC-2900, AC-3012, AC-4096), Polish 217, Polimer, Pretoria, Proud, Prudents, Raubkopie, Russian Group (311, 417, 516, 600, 696, 707, 711, 948, 1049, 2144, Mirror), Saddam, Scotts Valley, Sentinel 1, Shake, Slow, South African 1, South African 2, South African 416, Spanish, Spanish Telecom, Staf, Stardot-801, St. Petersburg, Subliminal, Sunday, Suomi, Suriv 1.01, Suriv 2.01, Suriv 3.00, SVC v3.1, SVC v4.0, Sverdlov, Svir, Sylvia, Syslock, Taiwan A, Taiwan B, Tenbyte, Terror, Testvirus B, The Rat, Tiny, Tiny Family 1 (T154, T156, T158, T159, T160, T167, T198), Tiny Family 2 (T133, T134, T138, T143) Traceback, TUQ, Turbo 488, Turbo Kukac, Twelve Tricks, Typo, V-1, V2000, V2P2, V2P6, Vacsina Family (TP04, TP05, TP06, TP16, TP23, TP24, TP25), Vcomm, VFSI, Victor, Vienna Family (1, 2A, 2B, 3, 4, 5A, 5B, 6A, 6B, 582, 644, 646, 774, 822), Violator, Virdem Generic, Virdem 1, Virdem 824, Voronezh, VP, Vriest, W13-A, W13-B, Whale, Willow, Wisconsin, Wolfman, XA-1 (1), XA-1 (2), Yankee Family (TP33, TP34, TP38, TP39, TP41, TP42, TP44, TP45, TP46), Zero Bug, Zero Hunt.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

PRODUCT REVIEW

Blue-Blooded DOS

Dr Keith Jackson

IBM has recently released *PC-DOS version 6.1*, which is being sold as a direct competitor to *Microsoft MS-DOS* (*VB*, May 1993, pp.17-19). Both operating systems include several add-on security features, including anti-virus and backup software. This review will look at these features of *IBM's PC-DOS* in their own right, but I will briefly attempt to contrast the two products' other properties.

Documentation

The review copy of *PC-DOS* was provided on five 1.44 Mbyte, 3.5-inch floppy disks. Lower density disks (720 Kbyte, 3.5-inch) are available free on request, but there is no mention of any availability of 5.25-inch disks. This is still better than *MS-DOS*, which arrived on 1.44 Mbyte disks, with no mention of *any* other disk formats.

The documentation states that updated versions of *IBM AntiVirus*, the built-in anti-virus software, are available free to purchasers of *PC-DOS*: one immediately, and one in 'three to four months'. An immediate upgrade is very useful, as it brings any product which has been lying on a dealer's shelf right up to date. After these first two upgrades, new virus signatures have to be purchased, but the fee is nominal (about £11.50). Very helpfully, the documentation lists upgrade details for various countries around the world. Everything is priced in both local currencies and Danish kroner (the upgrades are available from *IBM* in Denmark). All in all, this is well thought out.

The *PC-DOS v6.1* documentation is voluminous to say the least. It comprises a 28-page Installation Guide, a 390-page Command Reference & Error Messages book, a 426-page Users Guide, a 32-page Keyboards & Code Pages booklet, a 158-page Everyday DOS book (the 'Janet and John Guide to DOS' bit), and a 103-page Data Compression Guide.

I have no space in this short review to go into detail about the documentation. However, it is patently clear that a lot of effort has been expended on it, which has resulted in a thorough, readable, and easy-to-use manual. The README file which accompanies the documentation is 50 Kbytes long and bang up to date: the files on the *PC-DOS* disks were dated just nine days before the beginning of my tests!

Installation

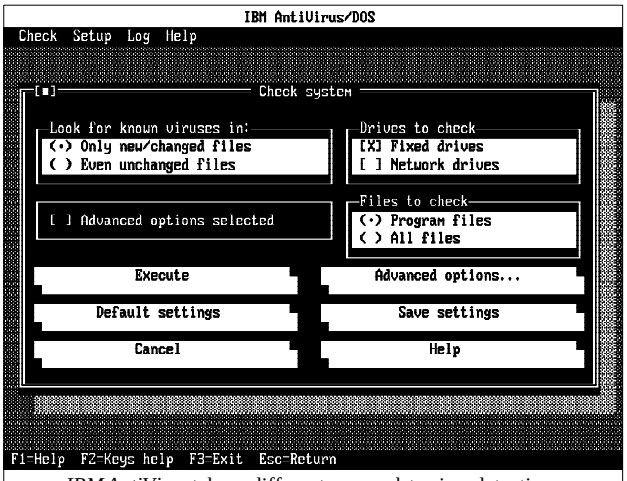
Installation of *PC-DOS* turned out to be very easy. During this process, a few system choices such as country, keyboard, and screen font have to be made, but sensible defaults are offered, and on-line help is always available by pressing the F1 key. In a similar vein, the user can choose whether utilities such as *IBM AntiVirus*, the backup/restore features, the DOS shell, PCMCIA support, *PenDOS* (for pen driven systems), and data compression are installed. The installation program makes it quite clear how much hard disk space will be occupied by each of these options, the worst cases being 6.5 Mbytes for all the DOS 'bells and whistles', and a whopping 15.5 Mbytes if every DOS and *Windows* feature is fully installed.

Once started, the actual installation process consists of nothing more than inserting floppy disks in the correct order, and then waiting for some time while a gargantuan hard disk thrash takes place at the end. Complex alterations are made to the start-up files AUTOEXEC.BAT and CONFIG.SYS (copies of the old files are preserved for future use). I was impressed to see that the installation program had been through these files very thoroughly, and changed every reference made to an old operating system feature into the appropriate new reference. Features such as a RAM drive, use of the 4DOS command interpreter, and the DOS shell program were all swapped for new versions, and worked straightaway with no problems whatsoever.

Overall, this version of *PC-DOS* scores equally with *MS-DOS 6* on ease of installation, but *PC-DOS* does seem to pay a little bit more attention to detail.

Anti-virus Features

The anti-virus software included with *PC-DOS v6.1* is called *IBM AntiVirus*. The first time that this is executed, the user is informed that it is 'initializing its database', during which time it searches through the entire hard disk to figure out which executable files are present. This takes quite a few minutes, but only happens at installation time. All subsequent executions simply make alterations to this database.



IBM AntiVirus takes a different approach to virus detection, combining the speed of a checksummer with the virus specific detection of a scanner.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

There are many different set-up options provided: for example, an automated virus check can be carried out (each boot, daily, weekly or monthly), the memory-resident anti-virus software can be installed (or not), high memory can be scanned, and desired combinations of drives/files can be specified. *IBM AntiVirus* does not have the myriad complex options supported by some products which I have reviewed, but what is on offer is perfectly adequate.

IBM AntiVirus is actually produced by none other than *IBM* itself. This contrasts with *MS-DOS v6* which includes a lightly disguised version of *Central Point's CPAV* program. Indeed, my review of *MS-DOS* made the point that apart from the different name, I was hard pushed to see many differences between the *Microsoft Anti-Virus* program and *Central Point's* original offering, including the bugs!

The Best of Both Worlds…

IBM AntiVirus can scan only those files which are new or unchanged (that is the point of the database), or 'even unchanged' files. Note that the last phrase is a quote from the *PC-DOS* documentation. The default mode of scanning is to inspect only files which the scanner thinks have changed since the previous scan. This obviously speeds up the scanning process (see figures below), but does have an associated risk. A virus which is capable of infecting an executable file, and then altering the entries in the *IBM AntiVirus* database in order to pass as unchanged, would neatly circumvent the program.

I have no doubt whatsoever that such a virus does not exist at this point in time, but I have less faith that one will not be developed at some future date. No doubt in an attempt to make life difficult for virus writers, the documentation does not explain exactly what the 'database' contains. This also has the side-effect that reviewers cannot comment on it.

In spite of the above caveat, I still believe that *IBM* has made a pragmatic attempt to incorporate some checksum (I assume) features into its scanner in order to produce a product which fits users' needs. Checksum programs which report every single bit change in every executable file are support-intensive, and frankly do not work at all well when executable files modify themselves routinely on execution (a practice which is becoming much rarer, thank goodness). Scanner programs which blindly search the rarely accessed corners of a hard disk are blundering through their search process for no reason. It does seem logical to try and combine the two methods, as long as it is done carefully.

Speed and Accuracy

IBM AntiVirus scanned the hard disk of my test computer, containing 891 files spread across 26.8 Mbytes, in 1 minute 9 seconds when scanning only new/unchanged files, and 4 minutes 55 seconds when scanning 'even unchanged' files. Note that this confirms the speed-up offered by the previously explained tactic of looking to see which files have changed, and only scanning the ones which have altered. Obviously, if many executable files have changed, then the minimum scan time of 1 minute 9 seconds quoted above will increase proportionately.

For comparison purposes, *Dr Solomon's Anti-Virus Toolkit* could scan the same hard disk in 1 minute 20 seconds, and *Sweep* from *Sophos* took 2 minutes 12 seconds in quick scan mode, and 8 minutes 28 seconds when doing a complete scan. Therefore, the *IBM AntiVirus* scanner is definitely one of the faster scanners around when it uses its tactic of scanning only those files which have changed since the last scan was performed. Considering that all files with the extension BAT, BIN, CMD, COM, DOS, DLL, EXE, OS2, OV?, PRG and SYS (far more than most scanners) are included in the *IBM AntiVirus* scan, the timings reported for 'even unchanged files' are still eminently reasonable.

Comparison with scan timings reported by *VB* in May 1993 for *MS-DOS v6* show quite clearly that the *IBM AntiVirus* scanner included with *PC-DOS* definitely outperforms the *Central Point* scanner included with *MS-DOS*, as far as speed of scanning is concerned, and by some margin.

The accuracy of virus detection provided by *IBM AntiVirus* was reasonable, but with some rather curious exceptions. The viruses which were detected can be split into two types - 'definite' and 'probable' virus infections. Strangely, the vast majority (84%, see below) of viruses were detected as only 'probable', even though they most certainly are viruses. I think (the manual is not clear on this point) that by 'definite', *IBM* means an infection by a known virus which can be disinfected. This point needs further explanation. I was intrigued to find that, as far as the Vacsina and Yankee viruses are concerned, some virus test samples are detected as 'definite', yet others are only 'probable'. Why?

"PC-DOS definitely outperforms the Central Point scanner included with MS-DOS, as far as speed of scanning is concerned"

Details of the virus samples used for testing are contained in the *Technical Details* section below. Of the 223 parasitic virus samples, 30 viruses were detected as definite infections, 184 as probable, and only nine samples went undetected. This corresponds to an overall detection rate of 96%. Due to the lack of a 5.25-inch drive on my test computer, the only boot sector virus which could be tested was Italian, which was detected. All the 1024 Mutation Engine samples were detected correctly.

The viruses which were not detected were Dark Avenger (a disturbing omission), three samples of Datacrime, and one each of Fu Manchu, Virus101, Power Pump and WinVir_14. By way of comparison, the *Central Point* scanner included with *MS-DOS* is almost, but not quite, as good: it failed to detect 10 viruses from a slightly smaller test-set. Attentive

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

readers will have noted that *IBM AntiVirus* achieved perfect scores in the latest comparative review. This is because the version shipped with *PC-DOS 6.1* is (according to the on-line help system) version 1.02: should the user send in the enclosed immediate upgrade card, the efficacy of the scanner is drastically improved, moving it well above *MSAV's* performance [*See page 15. Ed.*].

Shield

IBM AntiVirus offers a memory-resident feature called Shield DOS. I am unsure what this is actually doing, as the documentation merely says that 'If a virus is detected when you are running a program, you will be notified'. Other explanations are just as vague, and this really does warrant more explanation. I ran some timing tests whilst copying a large number of small files, and found that the time taken to carry out this exercise was the same, whether or not Shield was installed. This fits in with the fact that viruses can be copied when Shield is active, and no errors will be reported.

One other curious feature is that the documentation refers to a *Windows* version of *IBM AntiVirus*, but I cannot even find it. Given the newness of *PC-DOS*, this feature may of course have been omitted for marketing reasons. This is no major loss, as scanning for viruses when running *Windows* is rather missing the point. The *Windows* anti-virus program is even once referred to as *IBM AntiVirus DOS for Windows*, a name which is guaranteed to confuse users.

Backup

Included with *PC-DOS v6.1* is a version of *Central Point Backup*. This is the same software, bundled with *MS-DOS 6* and the *PC Tools* utility package. Versions for DOS and *Windows* are provided, and both seem to work reliably, with no obvious quirks.

One curious point is that although the DOS and *Windows* versions operate in a very similar manner, they seem to initialise themselves independently on their first execution. Perhaps I am being naïve, but I would have hoped that they would be aware of each other's presence, and let users switch seamlessly between the two. The *Windows* version in its default state (the Express interface) is particularly easy to use - just three huge buttons are visible on screen: Backup, Restore and Compare. Even the most computer illiterate user should be capable of figuring out what to do. Why can't all software be this easy to use?

Compression Software

PC-DOS v6.1 includes data compression software called *SuperStor/DS*, which is in direct competition with the *MS-DOS Doublespace* product. It even claims to be compatible with *Microsoft's Doublespace* - a statement which I could not think of any simple way to test. The documentation of *SuperStor/DS* is particularly well-written, including a very good section on what to do if things do go wrong, and an explanatory list of all error messages.

Inclusion of the name *SuperStor* within the *PC-DOS* compression software gives away the fact that this is another badged product, since the two best known hard disk data compression programs are called *Stacker* and *SuperStor*. Various commands are included to make *SuperStor/DS* easy to use, and I had no problem whatsoever with it.

Only time will tell if *SuperStor/DS* is reliable in operation. Certainly there has been none of the furore which occurred over the reliability of *Microsoft's* compression software - unlike *Doublespace*, *SuperStor* has been around for a long time, and has a proven track record.

Conclusions

I found *PC-DOS v6.1* to be a stable, well-documented product. The additional features offered by anti-virus software, decent backup facilities, and data compression should have been included in the operating system years ago. Comparisons of *PC-DOS 6.1* and *MS-DOS 6* are difficult to make as the products differ so much in fine details. They are roughly on a par as far as backup facilities and data compression software are concerned, but I prefer *IBM AntiVirus*: it is quite a bit faster in execution, and as shipped is marginally better at detecting viruses.

When I reviewed *MS-DOS* earlier this year, I concluded that including anti-virus utilities with the operating system could well send many anti-virus vendors to the wall. If *IBM's PC-DOS v6.1* is successful, I have no reason to change that conclusion. Subtle counter-arguments about the valid reasons for investing in a commercial anti-virus product will be a waste of breath: the crux of the matter is the success of *MS-DOS 6.0*. How many users have actually gone out and upgraded from version 5 of *MS-DOS*? To quote a well-known phrase, 'not a lot'.

Technical Details

Product: *PC-DOS*

Developer: *IBM*, who have contact points in nearly every country in the world.

Vendor: Most computer dealers.

Availability: An *IBM* true compatible with one 3.5-inch floppy disk drive, a hard disk with 4 Mbytes of available space, at least 512 Kbytes of RAM. The largest hard disk partition is 256 Mbytes. *Windows* version 3.1 is optional.

Version evaluated: 6.1

Serial number: None visible.

Price: £115 (or £45 if upgrading from an earlier version of DOS).

Hardware used: A *Toshiba 3100SX* laptop, which incorporates a 16 MHz 386 processor, 5 Mbytes of RAM, one 3.5-inch (1.4 Mbyte) floppy disk drive, and a 120 Mbyte hard disk.

Viruses used for testing purposes: This suite of 143 unique viruses (according to the virus naming convention employed by *VB*), spread across 228 individual virus samples, is the current standard test-set. A specific test is also made against 1024 viruses generated by the Mutation Engine (which are particularly difficult to detect with certainty).

For a complete listing of the viruses in the test-set used, see *Virus Bulletin*, August 1993, p.19.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

FEATURE

That was the Year...

1993 proved to be a busy year in the crazy world of the anti-virus industry. Products and companies have been born and have died, entire marketing campaigns have been contrived, run, and discarded, and the computer underground has continued to do its utmost to make life difficult for increasingly busy manufacturers. Some would say all this was merely business as usual!

Court and Social

The most eagerly awaited event of the 1993 anti-virus calendar was the launch of *MS-DOS 6*. Would *MSAV* be the product to provide anti-virus protection for the masses? Several months on, the answer appears to be no. *MS-DOS 6* was given a lukewarm reception by security experts: the virus detection rate was far too low, and concerns over the reliability of the built-in disk compression software forced *Microsoft* to rush out an 'upgrade', *MS-DOS 6.2*.

The promise of revenue from the inclusion of anti-virus software within DOS proved to be irresistible to the new-look *IBM*, which raced out with *PC-DOS 6.1* in the last quarter of the year. Will this product be the panacea for which the world has been waiting? Will other vendors suffer because of this latest release? Only time will tell.

The 1993 list of births, deaths and marriages makes interesting reading. *Symantec* has continued its minesweep through the anti-virus industry ('That company's mine, that one is mine…'), acquiring three virus scanners in rapid succession: *Certus NOVI*, and *Fifth Generation's Untouchable* and *Search and Destroy* products. Each of these scanners has since been withdrawn. *Central Point* has spent 1993 similarly occupied, reportedly happy with its recent takeover of *Xtree*.

The now customary January relaunch of *S&S International's* magazine, *VNI*, this year sees a change of name. *Virus News International* is dead: long live its latest mutation, *Secure Computing*! This new magazine will aim to fill the gap in the market for a glossy computer security publication. Any guesses as to what it will do in January 1995?

Spreading Slowly

If 1993's batch of viruses had one particular theme, it was polymorphism. By the end of the year, researchers had polymorphic viruses coming out of their ears! MtE, TPE, NED… the acronyms mounted up rapidly, leaving behind all those who were not prepared to burn the midnight oil. This has made testing rather difficult: due to the level of polymorphism involved, many thousands of samples are needed to guarantee accuracy, ensuring plenty of late nights.

The computer underground was meanwhile working on its next project: 'build your own virus' kits. These handy toolkits (now available in a number of different versions) allow completely inexperienced users to create their very own viruses. Using the kits, it is even possible to put in one's own customised trigger routine.

The good news was that there were no large virus outbreaks last year. 'Michelangelo Day' passed with a whimper rather than a bang (but it was on a Saturday), and the press was blissfully free of the 'computer Armageddon' type of story which had typified most articles on computer viruses.

Silence in Court?

Being a virus writer in 1993 turned out to be a hazardous pastime, as *New Scotland Yard's Computer Crime Unit* tore around England arresting unsuspecting hackers, battering down doors, and generally doing their best to bring computer criminals to justice. However, catching the criminal proved to be easier than gaining a conviction. In the spring of last year, Paul Bedworth was found 'not guilty' in the 'hacking trial of the decade.' Bedworth, despite admitting breaking into a number of different computer systems, walked free from *Southwark Crown Court*, much to the consternation of officers working on the case (and others!).

Not all of those nabbed by the long arm of the law were so lucky. A number of American hackers were convicted last year, most notably Joseph Popp of 'AIDS Disk' fame, who was finally 'brought to book' in Italy. It seems unlikely that Mr Popp will be extradited from the USA, but he would be extremely well advised to avoid any holidays in Rome for the foreseeable future.

Still awaiting trial for virus writing are members of the UK computer virus writing group, *ARCV*, although no court date has yet been set. It is hoped that 1993's list of arrests and convictions will convey the appropriate message to all hackers and virus writers.

The Undiscovered Country

The principal trend in the virus world is one of continued effort. The problem no longer attracts the sort of media attention it once did, but is still very much there: surveys show that both the number of known viruses and the number of viruses in the wild continue to grow. The fight for developers is to keep their products up to date, in the face of an increasingly well-organised computer underground.

New laws, and a heightened awareness of the real dangers to come will, in the long run, go some way towards helping the current situation, but the short term goals can only hope to be achieved by continued research. Virus developments look set to push scanners to their limits (e.g. Cruncher, or a combination of Commander Bomber and the Mutation Engine), and the next line of defence is not yet clear. Any prophecies on how the industry will look next January? Answers on a postcard to: The Editor, *Virus Bulletin*.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

ADVISORY BOARD:

Jim Bates, Bates Associates, UK
David M. Chess, IBM Research, USA
Phil Crewe, Ziff-Davis, UK
David Ferbrache, Defence Research Agency, UK
Ray Glath, RG Software Inc., USA
Hans Gliss, Datenschutz Berater, West Germany
Igor Grebert, McAfee Associates, USA
Ross M. Greenberg, Software Concepts Design, USA
Dr. Harold Joseph Highland, Compulit Microcomputer Security Evaluation Laboratory, USA
Dr. Jan Hruska, Sophos, UK
Dr. Keith Jackson, Walsham Contracts, UK
Owen Keane, Barrister, UK
John Laws, Defence Research Agency, UK
Dr. Tony Pitt, Digital Equipment Corporation, UK
Yisrael Radai, Hebrew University of Jerusalem, Israel
Roger Riordan, Cybec Pty, Australia
Martin Samociuk, Network Security Management, UK
Eli Shapira, Central Point Software Inc, USA
John Sherwood, Sherwood Associates, UK
Prof. Eugene Spafford, Purdue University, USA
Dr. Peter Tippett, Symantec Corporation, USA
Steve R. White, IBM Research, USA
Joseph Wells, Symantec Corporation, USA
Dr. Ken Wong, PA Consulting Group, UK
Ken van Wyk, CERT, USA

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

SUBSCRIPTION RATES

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, Oxfordshire, 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

This publication has been registered with the Copyright Clearance Centre Ltd. Consent is given for copying of articles for personal or internal use, or for personal use of specific clients. The consent is given on the condition that the copier pays through the Centre the per-copy fee stated on each page.

END NOTES AND NEWS

The IRA has unleashed a computer virus on the City of London, according to a report in the *Sunday Express*. The article goes on to explain that computer experts sympathetic to the terrorists have written a virus believed to be targeted at London's *Stock Exchange*. Does this spell the end of computing as we know it? Unlikely - the virus in question appears to be a crude Jerusalem variant, Jerusalem.IRA. The virus has been known to the research community for some time, and poses no more of a threat than any other. *VB* has received no reports which indicate that the virus is in the wild.

Roger Thompson looks set to announce a split with *Leprechaun Software*. Thompson, who has continued to develop *Virus Buster 3.xx*, instead of the company's latest release *Virus Buster 4*, said, 'We found that our aspirations had diverged to the point where it seemed reasonable to split the company.' *Virus Buster 3* will henceforth be known as *The Doctor*.

The number of laptops stolen from unsuspecting users continues to rise. However, to an industrial spy, the data on the machine is of far more value than the machine itself. In an attempt to combat this problem, *PC Guardian* has announced the *Universal Notebook Guardian*. The product is designed to provide protection by locking the 3.5-inch drive with a multi-strand steel cable which may be secured to a stationary object. For further information, contact Pauline Basaran. Tel. +1 (415) 459 0190.

According to the *National Computing Centre* (*NCC*), **only one in seven UK users follows security procedures to prevent viruses**, even after direct experience of virus infection. Launching its second survey of 10,000 firms in conjunction with the *Department of Trade and Industry* and *ICL*, the *NCC* said it hopes to increase awareness of IT security breaches. A similar survey was carried out in 1991, which concluded that more than half of businesses had suffered from IT security problems, at an estimated total cost of £1.1 billion a year. The findings of the new report are expected to be available in early 1994.

Micheal Lafaro, the owner of New York-based *MJL Design*, and John Puzzo, one of the firm's technicians, have been charged with **threatening to release a computer virus** at a customer site. Lafaro sold software to William Haberman in November. After complaining about the software, Haberman made only a partial payment. Haberman contacted the police: they told him to pay Lafaro the outstanding amount on condition that Puzzo removed the alleged virus. When he did so, he was arrested. Under tough new computer misuse laws in New York, the men could face a prison sentence of 15 years, three times maximum jail sentence under the UK's *Computer Misuse Act*.

Jim Bates has been elected as President of *The Institute of Analysts and Programmers*, Britain's leading professional body for computer programmers. The appointment reflects Bates' continued efforts to help both the Police and users who have been affected by computer crime. Speaking about the post, Bates commented, 'As computing becomes ever more complex, I hope I can help the *IAP* to continue its promotion of standards of ethical and technical behaviour which enable everyone to benefit from the use and development of computers.' [*Bow. Scrape. Ed.*]

Patricia Hoffman's *VSUM* Listings will be resumed next month, as *VB* has not received a copy of any results since October.

The *NCSA* has announced *IVPC '94*, the organisation's annual *International Virus Prevention and Information Security Conference*. The conference will be held at *Stouffer Concourse Hotel*, Washington DC, on March 31st - April 1st, 1994. Tel. +1 (717) 258 1816.

Open Networks Engineering has just announced a new range of products designed to provide secure data transfer. *SecurLAN*, the company's latest product, provides secure data transmission facilities as well as Access control features on both Local and Wide Area Networks. The product uses DES to ensure data confidentiality, as well as RSA. For further information, contact Jon MacDonough. Tel. +44 (0)279 870860.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.