ISSN 0956-9979 JULY 1997

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

IN THIS ISSUE:

• **Comparing thoughts.** July sees the second of *Virus Bulletin's* biannual DOS scanner reviews – were there any surprises from this year's motley crew? Turn to p.8 for the full story.

• **Wannabe.** What virus writers really really want is reflected in the latest EPO virus family to be analysed by *Virus Bulletin*. Beata Ladnai makes sense of the code used by the group; see p.6.

• **Editor's thoughts.** *VB*'s new editor, Nick FitzGerald, finally picked up his pen this month – read his opening gambit on p.2.

CONTENTS

EDITORIAL

Pawn to King-four…

As Ian did a few months ago, I have been looking through past issues of *Virus Bulletin* with a particular interest in ultimate and inaugural editorials. From what I have read, it seems that threats of serious legal action and being arrested (although apparently over unrelated matters!) are par for the course for the incumbent in this position. As neither are part of my stock of life experiences, it seems I can look forward to interesting times at *VB*!

And interesting times on the virus/anti-virus front too. The three out-going editorials have all touched on the rapid growth in the number of viruses, both in the wild and otherwise. When Edward Wilding started as *VB's* first Editor, there were fourteen known PC viruses – 42 months later, in his final editorial, he reported 'approaching (or exceeding) 3000'. Twenty-six issues later, Richard Ford threw in his pencil with the number around 6000, and after another 24 editions, when Ian traded HBs for C and *NT*, the number had grown to 10,500 or so. In the intervening few months, the number has blossomed to close to 12,000, boosted by continuing growth in the number of *Word* macro viruses (now reported at over 1000; see 'News', p.3).

"I have made one significant change at VB *already.."*

The issue of how virus families and variants should be counted has received quite some attention amongst anti-virus researchers recently: I feel there are anomalies between the currently received wisdom regarding macro viruses and the position generally settled on a few years ago to deal with seriously polymorphic viruses. As I have been a tad busy preparing for my move from New Zealand to the UK to work through the debate to my satisfaction, and as this is an issue much larger than can be adequately dealt with in an editorial, I may return to it in a future issue.

To hark back to the number of viruses question for a moment, it always interests me how much the total number of viruses is seen (or perhaps 'portrayed') as all-important, especially in press releases and other, largely mainstream, media coverage of 'the computer virus problem'. Vendors like to beat up press coverage to spawn sales leads, and woe betide the advertising department which launches a media blitz one day, only to be overshadowed by a competitor's claims the next! Does it really matter that Product Y claims to detect 23 more viruses than Product X, when the base number for these (puerile) comparisons is in the order of 12,000? I long for the day when the advertisers concentrate on the real issues – but I'm not holding my breath.

Independent anti-virus software testing is one of *VB*'s strengths, and I plan to maintain that during my tenure (and I would start work for *VB* during a DOS comparative month!). There are some interesting 'larger forces' at play in this arena too – the US-based *NCSA* has been running a certification program for a while now, the *Secure Computing Checkmark* is gaining momentum and *ITSEC* is (amongst other things) investigating how to set up, measure and maintain quality ratings of anti-virus software and its developers. Speaking of *ITSEC*, some of our readers may be interested in *ITSEC's* swished-up Web site mentioned in 'End Notes and News', p.24.

For those who do not 'know' me already (from Virus-L and comp.virus), I am afraid neither of holding opinions nor of taking stands based on those opinions. I prefer straight-shooting openness to scuttling around behind closed doors. I would like to hear what you think of VB, particularly now I'm Editor. Email is generally the best way to contact me – nick@virusbtn.com.

It is with some regret that within a week of disembarking from my flight to the UK I have had to say farewell to Megan Skinner – originally Editorial Assistant and for some time now Assistant Editor, she has left VB for an Editor's position at another magazine. Megan's mindful ministrations and Jakub Kaminski's technical expertise have largely been responsible for *VB* sailing on for the two-and-a-bit editions between Ian's departure and my arrival.

In closing my introductory editorial, I will just note that I have made one significant change at *VB* already, though probably only Edward, Richard and Ian will notice – and even then, only should they visit the office. Within half a day of starting I had to ditch that damn uncomfortable editor's chair! (Edward and Richard can fight Ian for it…)

NEWS

1000 Macro Virus Mark Passed

Early in June, anti-virus researchers reported that the number of known macro viruses passed 1000. Of the 300-odd families of such viruses, most only have one or two variants; however, a handful of families consist of many dozens of variants.

Viruses for MS Word versions 6 and 7 make up the vast bulk of known macro viruses. From the first 'in the wild' Word virus, Concept, in late 1995, the geometric growth to more than 1000 such viruses today has changed the way in which parts of the anti-virus industry operate. In the face of such growth, and of the speed with which new variants or strains can spread around the world via infected email attachments and Internet downloads, some vendors are moving to releasing 'hourly updates'.

While not updated literally every sixty minutes, some scanners' virus description databases are updated every time a new macro virus is added to the vendor's collection. In some cases, vendors update their macro virus descriptions half a dozen (and occasionally more) times per day.

As with other virus threats, the number of variants causing noticeable real-world incidents is a small fraction of the total – it would probably be generous to say 100 macro viruses account for most infections reported to researchers. However, the risk of any of the others 'taking off' as the result of a lucky break, such as being distributed to a worldwide mailing list in a document attachment, or being included on a promotional CD, means that Word users cannot be too cautious with new documents ▮

…and Still too Few Precautions

According to a poll taken at the US PC Expo, and sponsored by anti-virus developer Symantec, more than 50% of users do not update their anti-virus software on a monthly, or more frequent, basis; this despite the fact that 47% also reported having had a virus infection within the previous twelve months. Fifty-two percent of respondents were unaware that Symantec offers updates free to its customers.

'This new study verifies that we need to focus more aggressively on public awareness of virus threats and currency of virus protection,' said Enrique Salem, of Symantec's Security and Assistance Business Unit.

The need to provide adequate protection against the virus threat is underlined by the fact that the number of extant macro viruses is now in excess of 1000, up from only 42 in August 1996.

Information on the poll can be seen at the Symantec Web site; http://www.symantec.com/ ▮

Prevalence Table – May 1997

Virus	Type	Incidents	Reports
Cap	Macro	61	20.4%
Concept	Macro	44	14.7%
NPad	Macro	29	9.7%
AntiEXE	Boot	13	4.3%
Wazzu	Macro	13	4.3%
Form	Boot	11	3.7%
Parity_Boot.B	Boot	9	3.0%
DZT	Macro	8	2.7%
AntiCMOS	Boot	8	2.7%
NYB	Boot	7	2.3%
Empire.Monkey	Boot	5	1.7%
Laroux	Macro	5	1.7%
MDMA	Macro	5	1.7%
WelcomB	Boot	5	1.7%
EXEBug	Multi	4	1.3%
Ripper	Boot	4	1.3%
Sampo	Boot	4	1.3%
Johnny	Macro	3	1.0%
Stoned.Spirit	Boot	3	1.0%
Appder	Macro	2	0.7%
Bug70	Boot	2	0.7%
Colors	Macro	2	0.7%
INT10	Boot	2	0.7%
Junkie	Multi	2	0.7%
Lunch	Macro	2	0.7%
Michelangelo	Boot	2	0.7%
Quandary	Boot	2	0.7%
Shell.10634	File	2	0.7%
Showoff	Macro	2	0.7%
Others [1]		38	12.7%
Total		299	100%

[1] The Prevalence Table includes one report each of the following viruses: 2lines, Alien, Attack, Beryllium, Bleah.B, Bupt_9146, Chaos, Damnfog.1748, Date, Diablo, Die_Hard, DMT, Edwin, Goldfish, Hybrid, Joshi, Kaczor.mp.4444, Karnavali, Kompu, LBB_Stealth, NiceDay, One_Half, Oxana.1671, Quicky.1671, RAP, Satria, Spanska.1500, Stat, Stealth_Boot.C, Stoned, Stoned.Angelina, Swiss_Boot, Temple, Tentacle, Tequila.2468, Trojector, Turbo, Unashamed, and Urkel.

Readers are reminded that bookings are now being taken for VB'97, to be held in San Francisco on 2/3 October 1997. Contact the conference coordinator Alie Hothersall for details; Tel +44 1235 544034 or email alie@virusbtn.com ▮

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 15 June 1997. Each entry consists of the virus name, its aliases (if any) and the virus type. This is followed by a short description (if available) and a 24-byte hexadecimal search pattern to detect the presence of the virus with a disk utility or 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

Aiwed.852 **ER:** An appending, 852-byte virus, containing the text 'AIWED'. The virus is partially encrypted. Infected files have the word 0DEADh at offset 0012h.

```
Aiwed.852       B8AD DECD 2172 4BE8 2203 0E07 32C0 B96D 00BF 5403 FCF3 AA8C
```

Assignation.426 **ER:** An appending, 426-byte virus containing the text '386 Virus - by Qark/VLAD - 1996'. The virus makes use of the CPU's 32-bit registers. The 'Are you there?' call: EAX=564C414Dh ('DALV'), Int21h returns the value EAX=524F434Bh ('KCOR'). Infected files have the word 564Ch ('LV') located at offset 0012h.

```
Assignation.426 66B8 4441 4C56 CD21 663D 4B43 4F52 74D5 8CD8 488E D866 33FF
```

Bell.390 **ER:** A simple, appending, 390-byte virus. It beeps after infecting a new file. Infected files have the word 4A41h ('AJ') at offset 0012h.

```
Bell.390        B8BA BACD 213D CACA 744F B821 35CD 212E 891E 6201 2E8C 0664
```

Cool.929 **ER:** A simple, appending, 929-byte virus. Its 'Are you there?' call returns the value AX=C001h.

```
Cool.929        E93F 023D AD0E 750A B801 C0CF E941 01E9 3601 3D00 4B75 F550
```

DWBomk.607 **CR:** An appending, 607-byte virus, containing the text strings 'COMMAND.COM' and '"DWBoMK"'. The payload triggers on 17 January and overwrites the contents of the first hard disk. Infected files have the byte CFh at offset 0003h.

```
DWBomk.607      B440 8B1E 0B01 B95F 02BA 0001 CD21 B442 B000 8B1E 0B01 B900
```

Glacier.1196 **CR:** A stealth, inserting, 1196-byte virus containing the texts '[Glacier v0.1a]', 'Happy Birthday to Amy.', and 'Written by Ghost Shadow of TPVO at L.C.T.C.'. Infected files have the word 5347h ('GS') at offset 0003h.

```
Glacier.1196    B800 83CD 213D 8345 7578 B42A CD21 81FA 0D04 7537 81C6 C603
```

Halka.1000 **CN:** An appending, 1000-byte virus infecting one file at a time. It contains the text 'Este es el virus 786 Version 1 Echo por --> √¡x∑Γ [√xΓ]/A.H.D. HALKA/. Industria Argentina' Quemen al muñeco del `94!' and 'OHH NO, ME HA DESCUBIERTO!!!', which is displayed on 31 December.

```
Halka.1000      5B53 B440 B9E8 038D 960B 01CD 215B B43E CD21 6800 0158 FFE0
```

Hasta.884 **CN:** An appending, 884-byte virus infecting one file at a time. On 19 January it displays the text 'HASTA LUEGO LUKAS' and on the 18th of each month it shows the message: 'HAPPY BIRTHDAY KAIN'.

```
Hasta.884       B404 CD1A 81FA 1901 7402 7566 E8B2 00E8 D900 E814 01E8 BE00
```

Helga.666.B **CN:** An encrypted, appending, 666-byte, direct, fast infector. It contains the text 'WARNING: ALL DATA ON NON-REMOVABLE DISK DRIVE C: WILL BE LOST! Proced with Format (Y/N)? Yes Ok'. Infected files have the byte 90h ('É') at offset 0003h.

```
Helga.666.B     B952 0290 5252 8A57 3B90 32D0 8857 3B90 43E2 F3C3 60B4 2CCD
```

Hideous.1024.C **CER:** An appending, 1024-byte virus with a payload, triggering on the 25th of every month, and overwriting the contents of the first hard disk.

```
Hideous.1024.C  B440 B900 0483 06FC 0201 CD21 803E 0C03 0074 0C32 C0E8 3500
```

Intruder.2028 **EN:** An appending, 2028-byte direct infector containing the texts '????????EXE?', '*.EXE', '*.*', and 'Please Wait'. The payload triggers on 19 May and deletes files and sub-directories.

```
Intruder.2028   E8CB FFB9 EC07 33D2 8B1E FE00 B440 CD21 8B16 0501 8B0E 0701
```

Khiznjak.556 **CN:** An appending, 556-byte direct infector infecting one file at a time. It contains the text '*.com'. Infected files have their time-stamps set to 00:00:02.

```
Khiznjak.556    7256 BA10 01B9 2C02 908B 1E34 03B4 40CD 2172 45B9 0000 BA00
```

Lavi.843 **CR:** An encrypted, appending, 843-byte virus containing the texts '[USA 94] (c)1994 ANuBiS' and '-USA 94-'. Infected files have the byte 55h ('U') at offset 0003h.

```
Lavi.843        01CF BE18 01B9 3704 81E9 1801 268A 0234 5E26 8802 46E2 F5C3
```

Lavi.1460 **CR:** An appending, 1460-byte virus containing the texts '[LAVI 1.0] (c)1994 FaTHer MaC' and 'Hola… Tenga cuidado si piratea...Se puede contagiar algun virus.'. Infected files have the byte 4Ch ('L') at offset 0003h.

```
Lavi.1460       89F6 268A 0289 C080 EC00 3400 88DB 2688 0283 C200 83C3 0046
```

Light.1219

CEN: An appending, 1219-byte direct infector containing the texts 'This virus was made for Computer Virus Club 'Stealth' Our address : Kiev 148 - box 10' and '(c) Light General.Kiev.1995.For free use!' Infected files have the word 2424h ('$$') at offset 0003h.

```
Light.1219          BA00 01B9 C304 B440 CD21 33D2 2689 5515 2689 5517 C3B8 2012
```

LiquidPower.1016

CR: A stealth, encrypted, appending, 1016-byte virus containing the texts 'Liquid Power© Is A Dark Wizard 1996 Production' and 'Heloooo… I'm Very Very Sorry About Your HardDrive, But Was It Really Worth Existing.?. Soooo… Now It's Gone…(HAHAHAHAHA!!!) Oh, I almost Forgot… The HardDrive Is Allready Fucked Up Sooo Don't Try To Reboot… Greets To All Virii Makers! Liquid Power© 1996 Dark Wizard (Long Live Sweden)'. Infected files have the byte CCh at offset 0003h.

```
LiquidPower.1016    8D9E 1D01 B9C7 012E 8B86 FA04 2E31 0743 43E2 F958 595B C353
```

LostLove.853

CER: An encrypted, appending, 853-byte virus containing the text '[L0ST LOVE] by Murmandamus (prt2)' and 'Louise'. Infected files have their time-stamps set to 30 or 62 seconds.

```
LostLove.853        005D 81ED 1901 1E06 1E06 0E0E 1F07 BE30 0103 F58B FEE8 E602
```

Miny.218

CR: A simple, appending, 218-byte virus. Infected files have the byte 43h ('C') at offset 0003h.

```
Miny.218            E800 005E 83EE 03B8 3A4B CD21 0BC0 7440 8CC3 4B8E DBB8 0E00
```

Monster.421

CN: An appending, 421-byte direct infector containing the texts '*.*' and '*.COM'.

```
Monster.421         33C9 8BD1 CD21 B440 B9A5 018B D6CD 215A 59B8 0157 CD21 59E8
```

Northmens.815

CER: An encrypted, appending, 815-byte virus containing the text '[nORThMeNS aNGeR] Coded by C.A, Karlstad, Sweden, 10/96'. The virus avoids infecting some specific programs: *AN.*, *OT.* and *ND.* (e.g. SCAN.*, F-PROT.*, and COMMAND.COM).

```
Northmens.815       ??2E 8137 ???? 83C3 024F 75F5 EB0A E801 0000 C606 1F00 C3C3
```

Odious.569

CN: An appending, 569-byte, direct infector. It contains the texts '*.com', 'c:\chklist.*', 'c:\command.com', '????????COM', and 'The Creeper Virus V2.0'.

```
Odious.569          BA05 0103 D6B4 40B9 3902 CD21 B442 B900 00BA 0000 B000 CD21
```

Paz.2560

MCER: A multi-partite, encrypted, appending, 2560-byte virus containing the texts 'CHKLIST.*' and 'PAZ, por favor.'. When infecting the MBR of the first hard disk it stores the original MBR on track 0, but in an encrypted form. The virus recognizes itself in MBRs by the byte 24h ('$') at offset 0078h. The following two patterns detect the virus in files and memory, and in MBR and memory respectively.

```
Paz.2560            4A01 E807 0058 0500 01E9 4500 8BF0 B90B 0431 1C46 46E2 FAC3
Paz.2560            BDFE FF8E D8A1 1304 83E8 06A3 1304 B106 D3E0 408E C0FB 33DB
```

Permutan.544

CR: An appending, 544-byte virus containing the plain-text string 'Permutan'. The virus intercepts Int20h and infects only files invoking this interrupt. The payload randomly corrupts the BIOS low-level disk write procedure (decrements the number of sectors to be written).

```
Permutan.544        B43E CD21 2E8B 9C09 008B D6B9 2002 B440 CD21 7305 585A 59EB
```

QPA.256

CN: An overwriting, 256-byte virus containing the texts 'Insufficient system memory.' and 'Qpa-XX virus from FBIC:*.COM'. It stores the original 256 bytes in hidden, system, read-only files with the extension 'FBI'.

```
QPA.256             BA0F 02B9 0001 90B4 40CD 213B C172 23B4 3ECD 2172 1D5B 33C9
```

Rosebud.912

CE: An appending, 912-byte virus containing the text 'WARNING : This Rosebud virus is simple, because it was made for interest. But Next virus will be bit more complex.' It avoids infecting files named SCAN*.* and CLEAN*.*.

```
Rosebud.912         B800 7ACD 213D 7698 750F 2E8E 169E 012E 8B26 9C01 2EFF 2EA0
```

Rubbit.734

CR: An appending, 734-byte virus containing the text: '\RUBBIT.$$$'. The virus traces the Int21h chain.

```
Rubbit.734          A1E2 0303 C8BA 0010 B440 9CFF 1EC6 0358 B43E 9CFF
```

Sailor.1108

CER: An encrypted, appending, 1108-byte virus containing the texts 'Sailor.Mars', '-b0z0/iKx-' and 'OCANIFVITICSIV-FVABT'. The virus avoids infecting some anti-virus scanners and COMMAND.COM. Infected files have their time-stamps set to 28 seconds.

```
Sailor.1108         EC8B 5E04 8BEB 81ED 0300 2E80 BE47 0088 745B E802 00EB 560E
```

Steatoda

CER: Two prepending minor variants containing the plain-text string 'Steatoda' and other encrypted texts 'This file is infected by "Steatoda", you seem to have the 'protection, so... you will not be harmed by the virus. Press any key...' and 'C:\DAMAGE.MOR'. The 1623-byte variant corrupts infected .EXE files.

```
Steatoda.1455       B899 35CD 2181 FB99 9974 748D 9CE5 0143 2E80 77FF AA2E 807F
Steatoda.1623       B899 35CD 2181 FB99 9975 068D 9CFE 00FF E38D 9C04 0243 2E80
```

Wanderer.1756

CER: A stealth, appending, 1756-byte virus containing the texts 'HWF-TBCLCO2SCHKLIST.SMARTCHK ANTI-VIR' and ' HA!HA!HA! *[The WANDERER.II VIRUS 1995/02/10]* (c) Copyleft 9187-9192 by SVS / KOREA Shit!! Turbo Vaccine! sibal.. Kaesaekki!'. Infected files have their time-stamps set to 62 seconds.

```
Wanderer.1756       B0FF B40F 86E0 90CD 213D 0101 741B 33C0 8EC0 2681 3E54 006B
```

Zany.225

CN: An appending, 225-byte virus containing the text '.COM'. Infected files have the byte 2Ah ('?') at offset 0003h.

```
Zany.225            2D03 002E 8986 D900 B440 8D96 0400 B9E1 0090 CD21 B800 42E8
```

Zgenrat.785

CER: An appending, 785-byte virus containing the text 'ZGENRATN5'. Infected files have their time-stamps set to 0:00:00.

```
Zgenrat.785         E803 00E9 B2FE B911 03BA 0801 E82A 00C3 1F07 5D5F 5E61 2EFF
```

VIRUS ANALYSIS

What do SpiceGirls Want?

Beata Ladnai
Sophos Plc

It is widely thought that the days of DOS viruses are numbered in the wild, especially those parasitic viruses that do not infect boot sectors, do not make use of polymorphism, and do not propagate on newer, more popular, platforms. Their significance is fading despite their number, which is steadily increasing.

Though many dozens of new parasitic viruses emerge each month, very few of their authors leave the beaten track of virus writing. Only a small number of new viruses exploit 'good old DOS' in some unusual fashion. The SpiceGirl family of viruses belongs in this minority.

Classification

The SpiceGirl family (so far SpiceGirl-1440, -1451, -1619, -2123, and -2125) can be classified as Entry Point Obscuring viruses (see VB, June 1996, p.8), because they try to make identification of the viral Entry Point in infected files more of a challenge. EPO viruses usually achieve this by patching themselves into the middle of their targets.

EPO viruses use several different methods to find their hiding places. One method is to search files sequentially for a particular string of bytes which can be replaced (e.g. Simb-330 and Simb-333 look for a MOV AH, byte; Int 21h and replace it with a call to the virus). Another frequently-used technique is to trace the execution of the host code, in the hope of stumbling on an instruction that can be patched (for instance, Slug-872 modifies an E8h call). In such viruses, finding the appropriate location means extra effort for the virus, but also for virus scanners.

Nevertheless, the SpiceGirls do not make this extra effort; rather, they attempt to fool scanners before they dive into scanning the contents of a possibly-infected file.

Infected Files with Weird EXE Headers

The SpiceGirl viruses are resident COM infectors which convert the files they infect into EXE format. The simplest of the pentad, SpiceGirl-1440, is analysed here in some detail, to demonstrate how all the SpiceGirls take advantage of some unusual EXE header manipulations.

SpiceGirl-1440 is a prepending virus with a twist: the 5A0h virus bytes reside at the beginning of an infected file, and the initial 5A0h bytes of the host are appended to the file. A close look at the six-paragraph-long EXE header reveals the striking fact that the offset of the code segment in the load module is set to an apparently gibberish value, FFEAh. This 'weird' segment, relative to the beginning of the load module, can make sense if interpreted as the signed value -16h. Taking the entry point set to B2h, the initial CS:IP leads out of the load module without causing any hiccups to DOS – but it may create problems for scanners.

Once the program is loaded into memory, the first instruction processed hides at offset 52h in the PSP. This is the location of a fixed CBh byte (a RETF instruction), preceded by CDh 21h (Int 21) which together form the DOS function despatcher. The EXE header sets the stack pointer to the beginning of the load module so that the stack contains eight entries before execution starts.

Thus, when the virus kicks off with a RETF (far return) it will find a decent relocated far address (FFEAh + value of CS:B2h) on the stack. It is easily deduced that the destination of the jump is not really far away. In fact, control will stay at the RETF instruction. Because the stack (initially) contains seven instances of the same far address, the virus' initial far return instruction will loop to itself seven times. On the eighth time round this loop, the far return finds a different address on the stack, and control finally passes to the real entry point of the virus.

Installation

First, SpiceGirl-1440 calls Int 21h with AX set to 3053h in order to check whether it is already resident. If it is not, the virus allocates a block at the top of memory and copies itself there, building up an EXE file image of the virus.

As a copy of the EXE header is securely preserved at the end of the virus code, it is easily copied over the beginning of the image, followed by the initial stack content. The image is then completed by the whole copy of the virus, so it will (redundantly) contain the virus' EXE header again.

The finishing touch is to restore those far addresses in the built-up image which will be relocated when a file from the next virus generation is loaded into memory. To complete the installation process, the virus hooks Int 21h and jumps back to the beginning to repeat the 'Are You There?' call.

Execution of Host Programs

Repeating the installation check is unconventional. So is its outcome. With the virus resident, calling Int 21h function 3053h – instead of setting a register and returning quickly – causes the hooked function to take control.

The double-duty of this hooked function is to rebuild the host program from two fragments in memory and to give control to the original code. The same thing happens if the virus is already resident when an infected program makes the first 'Are You There?' call.

The Hooked Int 21h

With SpiceGirl-1440 present in the system, COM files will be infected on File Open (3Bh), File Mode Change (43h) and Execution (4Bh), and, in the case of SpiceGirl variants 2123 and 2125, also on File Rename (56h).

Before infecting any file, the virus hooks the Critical Error Handler (Int 24h) and checks that the name of the target does not end with ND.COM (COMMAND.COM, for example). Then it ensures that the first two bytes of the file do not match MZ or ZM, and checks the file size.

Files shorter than 5A0h or longer than EA60h bytes are left in peace, as are files with lengths a multiple of 200h or 3E8h. If the required conditions are met, the virus now prepends its code to the file (as explained earlier).

Anti-anti-virus Feature

Although all SpiceGirls are fairly simple parasitic viruses, they use many subtle ways to try and remain unnoticed. They disguise their memory block as a system block, and they are careful about preserving the original file date and attributes of infected files.

They also use a less straightforward technique: whenever an Int 21h call was required, the standard MOV AX, word1; Int 21h sequence was not used. Rather, the author used MOV AX, word2; XOR AX, 5347h; Int 21h (where 'word2' equals 'word1 XOR 5347'). This device may help escape heuristic detection.

Three of the five viruses (SpiceGirl variants 1619, 2123, and 2125) are encrypted, and the two longest variants have a feeble, but unusual, stealth feature. During the execution of an infected file, the resident virus can create a temporary file which contains the clean host program. However, this file is created only if the host file is opened during execution and the file name passed to File Open matches that in the current environment block.

The hooked File Open will return a handle to the (temporary) file, so the uninfected file content will show up on demand. The temporary file is immediately deleted when the original file should be closed. Thus, the stealth functionality is quite limited; it affects only the infected file currently being run. This could be an attempt to bypass 'have I been modified?' self-checks.

With all these features, members of the SpiceGirl family remain simple parasitic viruses without serious armour or payload. They are meticulously written but merely replicate, and probably would not spread in the wild. Indeed, perhaps they were not intended to make it in the wild.

What SpiceGirls Really Really Want...

…is to cause virus-scanners headaches. The essence of their 'spicery' is their entry point trickery. When scanning EXE files, the obvious step for scanners is to look at the code at the Program Entry Point. In the case of an infection by a SpiceGirls variant, this technique does not work. The recorded entry point is not located in the file, but only exists when the infected file is loaded for execution. As this cannot be an option for scanners, the anti-virus industry is forced to approach the SpiceGirls from a different angle.

SpiceGirls

Variants: SpiceGirl 1440, 1451, 1619, 2123, and 2125

Type: Resident COM infectors. Infected files are converted into EXE format. Variants 1619, 2123, and 2125 are encrypted.

Self-recognition in Files:

Re-infection is impossible, as files beginning with 'MZ' remain unaffected.

Self-recognition in Memory:

Int 21h, AX=3053h. This installation check function is responsible for executing the host.

Hex Patterns:

SpiceGirl-1440 in Files and in Memory:

```
C706 F100 0800 BEF2 05BF 0001
B996 00AC AAE2 FCBE 9601 B90A
```

SpiceGirl-1451 in Files and in Memory:

```
C706 F100 0800 BEFD 05BF 0001
B996 00AC AAE2 FCBE 9601 B915
```

SpiceGirl-1619 in Memory:

```
C706 F100 0800 BE0E 06BF 0001
B99C 00AC AAE2 FCBE 9C01 B9B7
```

SpiceGirl-2123 in Memory:

```
C706 F100 0800 BE51 08BF 0001
B99C 00AC AAE2 FCBE 9C01 B9AF
```

SpiceGirl-2125 in Memory:

```
C706 F100 0800 BE53 08BF 0001
B99C 00AC AAE2 FCBE 9C01 B9B1
```

SpiceGirl-1619, -2123, -2125 in Files:

```
0100 EAFF 7601 5347 B200 EAFF
1C00 0000 7801 EAFF 7C01 EAFF
```

Intercepts: Int21h, functions 3Dh, 43h and 4Bh. SpiceGirls-2123 and -2125 also intercept functions 3Fh and 56h.

Payload: None.

Removal: It is safest to replace infected files from clean backups, or to reinstall them from original distribution media.

COMPARATIVE REVIEW

Into the Valley of DOS

Phil Crewe

It's that time again. *VB* ventures where angels fear to tread – into the world of DOS scanner benchmarking. Whilst becoming less important in the ever-more-dominant world of *Windows*, the core product of any anti-virus developer is still the command-line scanner. Having said that, more of the products are providing a very *Windows*-like front end to the engine, probably foremost amongst them being *Anyware Antivirus.*

Not to deny usability issues and their importance, this review concentrates on the technical competence of the scanners, rather than on their look and feel. The focus here is really on speed and detection rates.

The review was carried out on a Pentium machine with 32MB RAM for the speed tests. Smartdrive was not installed, and the system was very plain-vanilla. Some of the other testing was carried out on a 486DX2, where speed comparisons were not required. Hence, the inherent sluggishness of the 486 as compared with the Pentium made no material difference.

In the Wild samples were tested singly, but in general other sample sets (Standard, Polymorphic and Macros) were tested in batches to streamline the process as much as possible. Naturally, the boot sector viruses were tested singly, with one 1.44MB 3.5-inch floppy infected with each virus in the test-set, and each floppy individually scanned. In all cases, the file samples were held on a CD-ROM and before each set of tests, new sets were downloaded to the hard disk of the machines concerned. For testing, the floppy disks were permanently write-protected and occasionally randomly checked to ensure that readability of the floppy was not degrading.

The boot sector test-set has grown, and now includes 90 viruses. No automated disk-changing mechanism was employed, and instead I have to state here my thanks to my wife Janet for doing most of the floppy disk testing and changing. It may be the only reliable way of doing the test, but it is certainly very tedious.

The speed test again comprised 5500 files on CD, occupying 552,992,768 bytes. Whilst this is used as a false-positive test, it has to be said that all the products did extremely well here – indeed, most of the software did not even register a single false positive. Reliability is certainly on the up. In each test, the conditions were duplicated, even down to restarting the machine between tests to ensure clean systems. Once again, each test was run twice to pick out systems which checksum the data on a first run: this increases the time taken, but subsequent runs are thus much quicker.

The final tests were against two floppy disks, each holding 43 files. One disk was clean but the files on the other were all infected with the Natas virus. This allows a comparison of scanning speed in clean and infected conditions.

The scanners were tested against the usual *Virus Bulletin* test-sets: In the Wild Boot, In the Wild File, Standard, and Polymorphic. The Standard virus test-set now comprises 774 samples of 321 viruses; the polymorphic, 13,000 samples (500 each of 26 viruses); and the In the Wild set, 527 samples of 147 viruses.

The new test-set added for this comparative review is the Macro virus set, which comprises 710 samples of 185 macro viruses. This last set contains infected DOC and DOT files (for Word viruses) and XLS files (for Excel).

However, the inclusion of macro viruses in the test-sets for a DOS scanner review raises some problems. Four of the tested products have very limited or no macro virus detection capabilities, but 'compensate' for this by providing separate scanners specializing in macro viruses. Whilst these stand-alone macro scanners work well, they complicate the collection and reporting of performance data for tests such as used in these reviews. The approach taken here is that for tests against the In the Wild sets only the performance of the 'main' scanner is reported. For the test against the Macro set the dedicated macro scanners' results are presented and this is noted in the commentary.

I certainly hope the developers of these products will soon follow the lead of their competitors and incorporate macro virus scanning into their standard scanners.

[*Editor's note:* PER Systems *also submitted a product for review; however, it could not be fairly tested, as all instructions were in Spanish. We hope to be able to include it in the next comparative review.*]

Alwil AVAST! v7.70 28 April 1997

ItW Boot	100.0%	ItW File	99.3%
ItW Overall	99.6%	Standard	100.0%
Polymorphic	88.5%	Macro	95.8%

AVAST! continues to do well in the In the Wild and Standard sets, particularly so with the boot sector and wild file samples. The only virus it missed from the In the Wild set was an Excel macro virus, Laroux.A, which is also reflected in the lower macro detection rate.

It has, however, deteriorated slightly on the polymorphics, missing all samples of the Baran.4968, Cryptor.2582 and Mad.3544 stems, although it does detect every variant of all other stems.

	ItW Boot		ItW File		ItW Overall	Standard		Polymorphic		Macro	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil AVAST!	90	100.0%	523	99.3%	99.6%	774	100.0%	11500	88.5%	680	95.8%
Anyware Antivirus	79	87.8%	225	44.6%	61.0%	392	61.5%	155	0.9%	366	51.1%
Cheyenne InocuLAN	89	98.9%	516	98.0%	98.3%	768	99.3%	11482	86.4%	585	82.2%
Command F-PROT	90	100.0%	515	97.8%	98.6%	678	91.0%	7050	50.3%	695	97.8%
Cybec VET	90	100.0%	418	81.0%	88.2%	654	88.9%	12482	95.1%	691	97.3%
Data Fellows F-PROT	90	100.0%	494	93.7%	96.1%	678	91.0%	7050	50.3%	694	97.3%
DialogueScience DrWeb	85	94.4%	394	76.2%	83.1%	359	47.3%	12000	92.3%	658	93.0%
Dr Solomon's AVTK	90	100.0%	527	100.0%	100.0%	774	100.0%	12884	98.4%	702	98.9%
EliaShim ViruSafe	86	95.6%	523	99.3%	97.9%	774	100.0%	11500	88.5%	604	84.7%
ESaSS ThunderBYTE	90	100.0%	527	100.0%	100.0%	751	97.8%	12546	93.5%	695	97.8%
H+BEDV AVE32B	56	62.2%	499	94.2%	82.1%	644	88.4%	8273	33.0%	670	94.1%
H+BEDV AVSCAN	86	95.6%	511	96.8%	96.3%	652	88.3%	10143	74.9%	560	78.0%
IBM AntiVirus	90	100.0%	527	100.0%	100.0%	773	99.7%	12000	92.3%	685	96.2%
Intel LANDesk	84	93.3%	501	95.8%	94.8%	468	71.7%	10948	81.4%	428	60.5%
Iris AntiVirus	90	100.0%	526	99.7%	99.8%	766	99.0%	11479	86.4%	589	82.7%
KAMI AVP	90	100.0%	526	99.7%	99.8%	716	94.4%	12497	95.2%	641	90.3%
Look Software Virus ALERT	88	97.8%	412	80.3%	86.9%	635	87.3%	11349	80.9%	498	67.3%
McAfee VirusScan	90	100.0%	525	99.6%	99.7%	750	98.0%	12286	90.1%	706	99.5%
Norman Virus Control	90	100.0%	527	100.0%	100.0%	669	92.2%	11483	87.4%	703	99.1%
SafetyNet VirusNet	90	100.0%	494	93.7%	96.1%	678	91.0%	7050	50.3%	255	36.5%
Sophos SWEEP	90	100.0%	527	100.0%	100.0%	772	99.7%	13000	100.0%	710	100.0%
Stiller Integrity Master	83	92.2%	474	92.3%	92.3%	519	77.4%	4082	26.4%	525	73.7%
Symantec Norton AntiVirus	90	100.0%	523	97.6%	98.5%	593	84.4%	10998	83.6%	677	94.3%
Trend PC-cillin	86	95.6%	520	98.7%	97.5%	467	71.4%	10850	80.9%	529	73.4%

Anyware Antivirus v3.00 5 May 1997

ItW Boot	87.8%	ItW File	44.6%
ItW Overall	61.0%	Standard	61.5%
Polymorphic	0.9%	Macro	51.1%

This is the first appearance of *Anyware Antivirus* in our bench-test feature; unfortunately, what it brings in terms of user interface is let down in terms of success. Its score against the In the Wild test-set was depressed by its problems with macro viruses, though it must be said that it also had problems with normal file viruses. Further, it failed to detect most polymorphic samples, and of those it did detect, only between 1% and 10% of each stem was found.

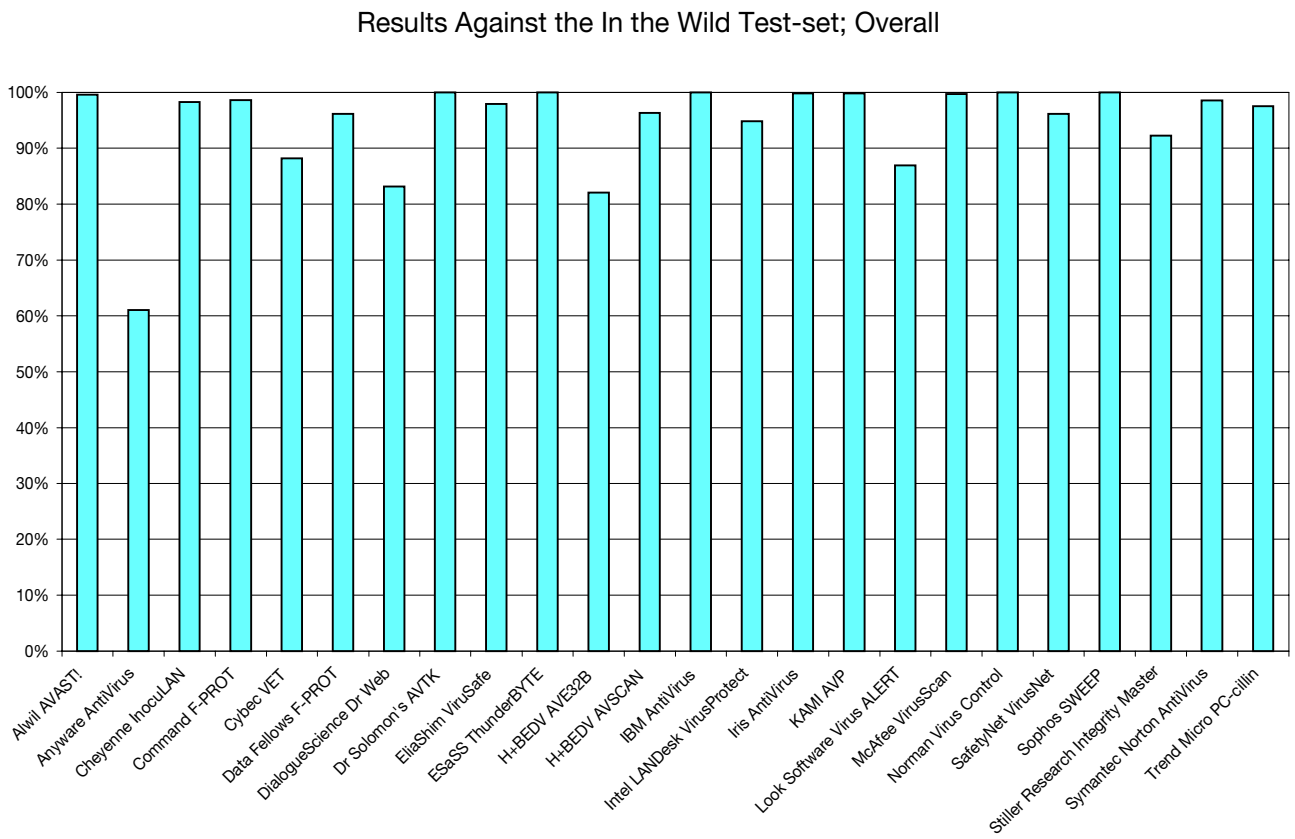
The product also encountered problems with the boot sector virus BootEXE.451, which caused a machine crash every time it was tried. Further, the Yankee_Doodle.2901 virus caused a machine freeze, despite correctly identifying the presence of the virus.

Cheyenne InocuLAN v4.0j 24 April 1997

ItW Boot	98.9%	ItW File	98.0%
ItW Overall	98.3%	Standard	99.3%
Polymorphic	86.4%	Macro	82.2%

A reasonable showing by *InocuLAN* this time, improving somewhat on its last review. However, it still does not detect all of the In the Wild test-set, and therefore remains a slight disappointment. *InocuLAN* should be a product which is up with the best, but at the moment it is slightly off the pace in this regard.

It missed a copy of Ornate in the boot sector set, plus the Hybrid.A *Word* macro, and some of the No_Frills.Dudley, Scitzo and Goldbug wild samples. It also shows general weakness against macro viruses, although its detection of wild macro viruses is reasonable. *InocuLAN* scanned the infected diskette surprisingly quicker than the clean one, but was amongst the slowest on the clean hard drive test.



Command F-PROT v2.26 April 1997

ItW Boot	100.0%	ItW File	97.8%
ItW Overall	98.6%	Standard	91.0%
Polymorphic	50.3%	Macro	97.8%

Command F-PROT seems to be making no progress in the bench-test scoring, still showing well in the Wild and Standard sets, but very weak in the Polymorphics. It missed Plagiarist.2051 and three *Word* macro viruses from the ItW File set, and almost half (5950) of the 13,000 polymorphic samples. The stand-alone macro virus scanner does creditably well against *Word* and *Excel* macro viruses. It does not recognise *Word 8* format files, but does inform the user of this when trying to open such a file.

The name of the *F-PROT* virus detection engine is generally good, and it shows some quite reasonable results when pitted against the Wild sets; however, some work must still go into the engine as regards detection of polymorphic viruses.

Cybec VET v9.40 April 1997

ItW Boot	100.0%	ItW File	81.0%
ItW Overall	88.2%	Standard	88.9%
Polymorphic	95.1%	Macro	97.3%

VET's failing against the Wild sets is wholly due to the inability of the main scanner to detect macro viruses. In most other respects *VET* turned in an excellent performance; amongst the Polymorphic set it only missed some of the Mad.3544 replicants and all 500 samples from the Cryptor.2582 stem.

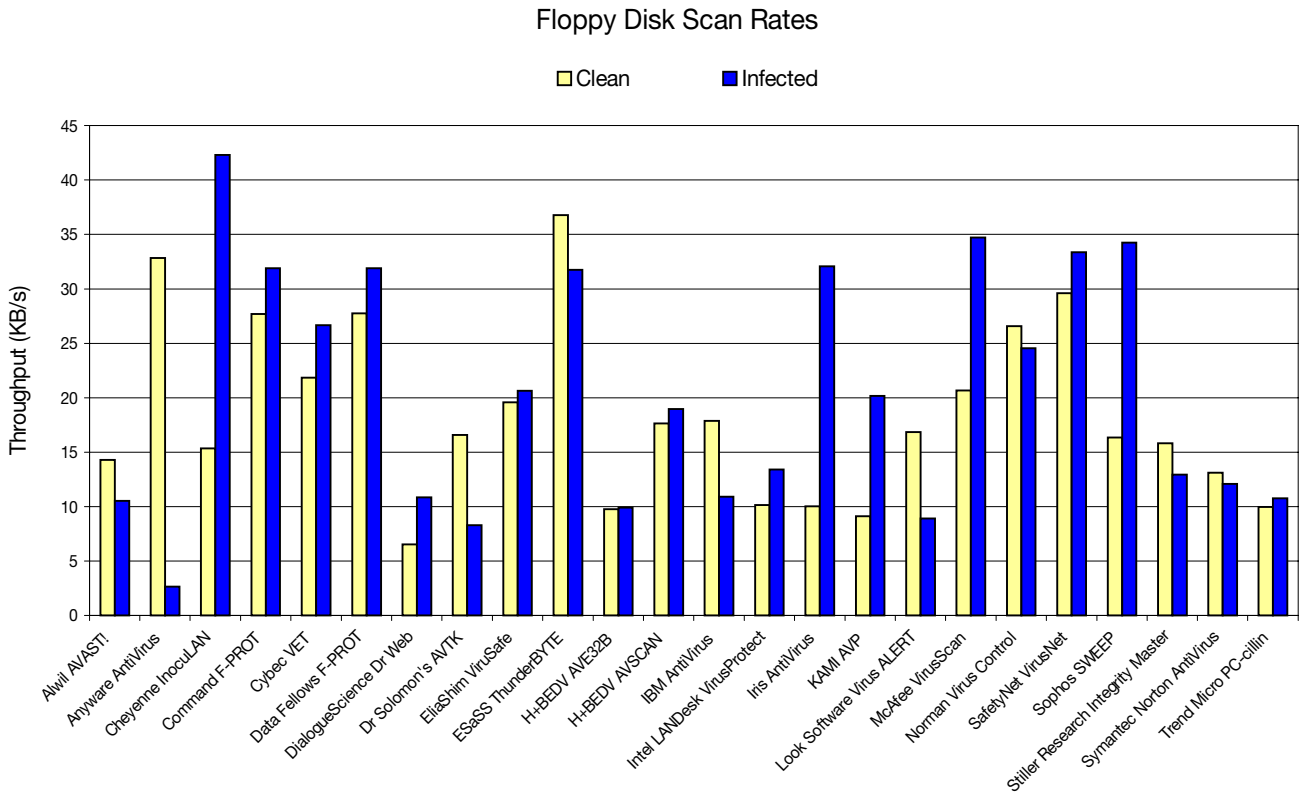
The separate macro virus scanner shipped with *VET* turns in a good performance. It is a pity that the engine has been split in this fashion, and I would encourage the merging of the two engines. This product does not support *Word 8* files, but a warning is given when it attempts to open one.

Data Fellows F-PROT v2.26 March 1997

ItW Boot	100.0%	ItW File	93.7%
ItW Overall	96.1%	Standard	91.0%
Polymorphic	50.3%	Macro	97.3%

The *Data Fellows* version of the *F-PROT* package shows extremely good detection capabilities against the In the Wild and the Standard virus test-sets, but is disappointing against the Polymorphics, missing many completely and others partially.

The separate *Data Fellows* macro scanner shows similar results to the *Command* version, but missed Divina.E – this may reflect the fact that *Data Fellows* supplied an older revision of the scanner. It also displays an error message when trying to open a *Word 8* file. I encourage the *F-PROT* developers to incorporate their macro scanner engine into their standard scanner to provide a more unified product and to avoid potential confusion.



DialogueScience Dr Web v3.21 29 April 1997

ItW Boot	94.4%	ItW File	76.2%
ItW Overall	83.1%	Standard	47.3%
Polymorphic	92.3%	Macro	93.0%

As in the last DOS comparative review, this product shows good performance against polymorphic and macro viruses, but is let down by poor detection of the supposedly easier Standard file viruses. Against the In the Wild test-set, it missed 133 of the 527 samples – 35 of the 147 viruses. One area where it certainly shone was its pure speed, clocking the fastest data rate on the clean floppies and on both runs against the clean hard drive.

Dr Solomon's AVTK v7.71 April 1997

ItW Boot	100.0%	ItW File	100.0%
ItW Overall	100.0%	Standard	100.0%
Polymorphic	98.4%	Macro	98.9%

Once again a brilliant showing by *Dr Solomon's Anti-Virus Toolkit*, which missed only 116 of the 13,000 polymorphic samples and eight of the 710 macro samples. This is a real improvement on last time's showing, probably due to the fact that the company shipped the latest version of the product this time around! The scanning speed is also extremely good. One of the two picks of the bunch, alongside *Sophos SWEEP*.

EliaShim ViruSafe v7.4 April 1997

ItW Boot	95.6%	ItW File	99.3%
ItW Overall	97.9%	Standard	100.0%
Polymorphic	88.5%	Macro	84.7%

ViruSafe missed the boot sector viruses Crazy_Boot, Hare.7750, Moloch and RP. However, missing only the *Excel* macro virus Laroux.A from the In the Wild File set bolstered its overall Wild score. With 100% detection of the Standard set *ViruSafe* was looking to be a very top contender, but this hope was let down somewhat by scores below 90% against both the Polymorphic and Macro sets. It does, nevertheless, show good scanning speed.

ESaSS ThunderBYTE v8.00 28 April 1997

ItW Boot	100.0%	ItW File	100.0%
ItW Overall	100.0%	Standard	97.8%
Polymorphic	93.5%	Macro	97.8%

This product shows an improvement on the In the Wild sets in this review, although a slight drop off in other areas summarizes *ThunderBYTE's* performance this time. It missed 23 samples in the Standard set, 15 in the Macros, and spotted all polymorphic families, although it missed some samples of Cryptor.2582, Girafe:TPE, Mad.3544, and SMEG_V0.3. Speed, however, was very good: *ThunderBYTE* was, as always, one of the fastest scanners in the test.

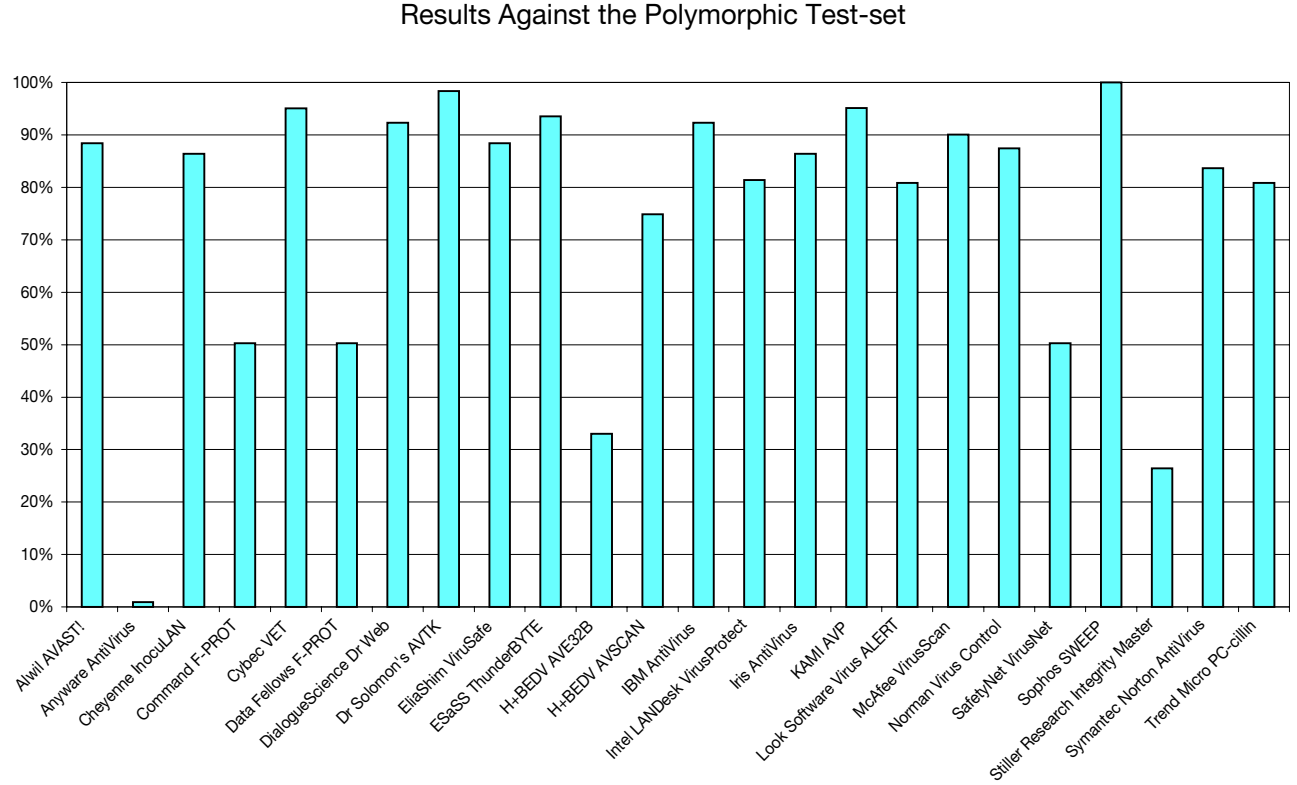
	Clean Floppy		Infected Floppy		Clean Hard Drive 1		Clean Hard Drive 2	
	Scan time (min:sec)	Data rate (KB/s)	Scan time (min:sec)	Data rate (KB/s)	Scan time (min:sec)	Data rate (KB/s)	Scan time (min:sec)	Data rate (KB/s)
Alwil AVAST!	1:08.2	14.3	1:52.2	10.5	7:00.7	1283.6	7:00.5	1284.4
Anyware Antivirus	0:29.6	32.8	7:22.5	2.7	8:28.2	1062.7	8:13.1	1095.3
Cheyenne InocuLAN	1:03.4	15.4	0:28.0	42.3	13:25.9	670.1	13:25.7	670.3
Command F-PROT	0:35.2	27.7	0:37.1	31.9	4:41.2	1920.2	4:40.9	1922.2
Cybec VET	0:44.6	21.8	0:44.3	26.7	15:51.6	567.5	3:16.2	2751.9
Data Fellows F-PROT	0:35.1	27.7	0:37.1	31.9	3:54.0	2307.5	3:54.0	2308.0
DialogueScience DrWeb	2:29.1	6.5	1:48.8	10.9	1:13.6	7339.4	1:13.5	7350
Dr Solomon's AVTK	0:58.8	16.6	2:22.4	8.3	4:02.7	2225.0	4:02.8	2224.5
EliaShim ViruSafe	0:49.7	19.6	0:57.3	20.6	3:25.6	2626.1	3:21.6	2678.3
ESaSS ThunderBYTE	0:26.5	36.8	0:37.2	31.7	1:27.1	6197.3	1:27.3	6183.1
H+BEDV AVE32B	1:39.7	9.8	1:59.4	9.9	5:14.7	1715.9	5:14.8	1715.6
H+BEDV AVSCAN	0:55.2	17.6	1:02.3	19.0	5:34.2	1615.8	5:34.3	1615.3
IBM AntiVirus	0:54.5	17.9	1:48.5	10.9	5:19.1	1692.1	5:19.3	1691.1
Intel LANDesk	1:36.1	10.1	1:28.3	13.4	9:38.9	932.8	9:38.9	932.8
Iris AntiVirus	1:37.1	10.0	0:36.9	32.1	11:52.7	757.8	11:52.5	758.0
KAMI AVP	1:46.9	9.1	0:58.6	20.2	10:29.5	857.9	10:30.0	857.2
Look Software Virus ALERT	0:57.8	16.8	2:12.6	8.9	4:34.7	1965.7	4:34.9	1964.5
McAfee VirusScan	0:47.1	20.7	0:34.1	34.7	12:15.4	734.3	12:15.5	734.2
Norman Virus Control	0:36.6	26.6	0:48.1	24.6	5:33.4	1619.8	5:33.3	1620.4
SafetyNet VirusNet	0:32.9	29.6	0:35.4	33.4	4:42.5	1911.8	4:42.5	1911.8
Sophos SWEEP	0:59.6	16.3	0:34.5	34.3	9:04.9	991.1	9:05.2	990.4
Stiller Integrity Master	1:01.5	15.8	1:31.3	12.9	6:58.9	1289.1	6:14.3	1442.7
Symantec Norton AntiVirus	1:14.1	13.1	1:37.9	12.1	6:30.9	1381.7	6:26.8	1385.6
Trend PC-cillin	1:37.9	10.0	1:49.9	10.8	21:57.4	409.9	21:59.3	409.3

H+BEDV AVE32B v5.08

ItW Boot	62.2%	ItW File	94.2%
ItW Overall	82.1%	Standard	88.4%
Polymorphic	33.0%	Macro	94.1%

H+BEDV submitted two products for review – their original *AVSCAN* is described below. Unfortunately, this was a poor showing first time out for this new package. It missed 34 of the 90 boot samples and 28 of the 527 In the Wild File samples. However, it shows much-improved performance over its stablemate in the Macro set, which probably reflects work being put into the new engine to detect later variants of macros.

As with *AVSCAN*, scanning speed was neither startling nor disappointing, however, *AVE32B's* floppy scanning is noticeably slower than *AVSCAN's*.



H+BEDV AVSCAN v3.42

ItW Boot	95.6%	ItW File	96.8%
ItW Overall	96.3%	Standard	88.3%
Polymorphic	74.9%	Macro	78.0%

AVSCAN performed about the same as in the last DOS comparative; improving slightly on the ItW test-sets, but faring slightly worse on the Standard and Polymorphic sets.

It missed ItW Boot samples of Cruel, Defo, Hare.7750 and Paula_Boot. ItW File samples of Plagiarist.2051, Goldbug, Mange_Tout.1099 and Ear.Leonard.1027, and the *Word* macro virus Hybrid.A, were also not detected. It is to be hoped that *AVE32B's* macro detection can be combined with *AVSCAN's* strengths and polymorphic detection beefed-up.

IBM AntiVirus v2.5.2 April 1997

ItW Boot	100.0%	ItW File	100.0%
ItW Overall	100.0%	Standard	99.7%
Polymorphic	92.3%	Macro	96.2%

As usual, an excellent performance from IBM in our tests. It is a pity that this product is less widely publicized, as it deserves a better reputation. It only missed Argyle from the Standard test-set, seven of 185 macro viruses, and all of the Cryptor.2582 and Mad.3544 polymorphs.

This certainly was not the fastest-scanning product, but if the checksumming routines are enabled, it can be tuned to give very good results in normal implementations.

Intel LANDesk v3.0r22 23 Oct 1996

ItW Boot	93.3%	ItW File	95.8%
ItW Overall	94.8%	Standard	71.7%
Polymorphic	81.4%	Macro	60.5%

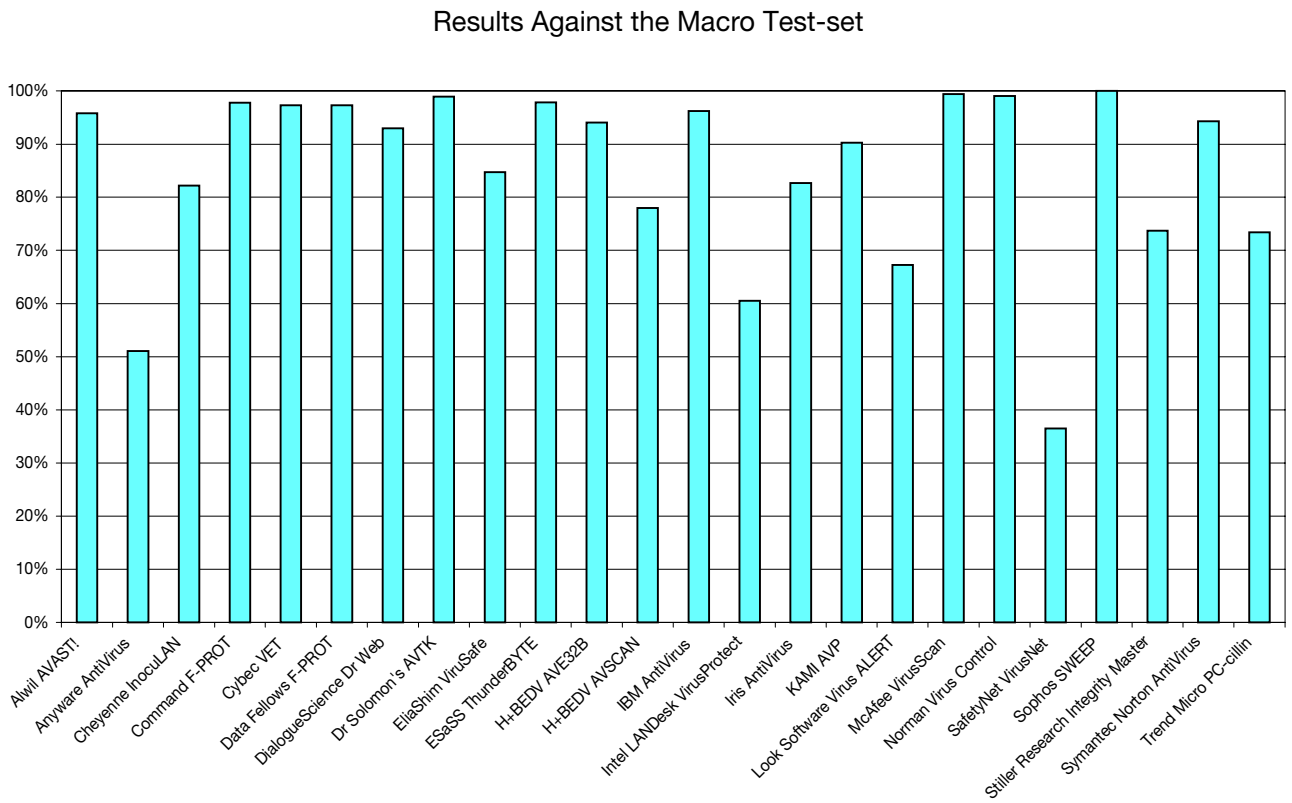
Similar results to those in our last DOS comparative. Not detecting all In the Wild viruses is still a worry. It missed six boot viruses; Hare.7750, Moloch, Neuroquila, Ornate, RP and Cruel; 26 of the 527 ItW File viruses; 16 macro viruses; plus Scitzo and two samples of each of the Hare 7610 and 7750 variants. The similarity between these and the last results may be due in part to a seemingly out-of-date virus data file.

Iris AntiVirus v21.36 30 April 1997

ItW Boot	100.0%	ItW File	99.7%
ItW Overall	99.8%	Standard	99.0%
Polymorphic	86.4%	Macro	82.7%

Again, a very impressive showing by this product. Whilst the user interface may be a little spartan, the engine is effective, and that remains the best test in this case. It only missed one of the two samples of No_Frills.Dudley from the Wild set, though it completely missed Baran.4968, Cryptor.2582 and Girafe:TPE, 17 of the DSCE.Demo replicants from the Polymorphic test-set, and 32 of the 185 macro samples.

For such a little-known product, this is a good showing in our tests, and it really should do better commercially.



KAMI AVP v3.0 28 April 1997

ItW Boot	100.0%	ItW File	99.7%
ItW Overall	99.8%	Standard	94.4%
Polymorphic	95.2%	Macro	90.3%

Another good showing for this product, although it still does not quite attain the 'unbeatable' reputation it once had. Like many other products, its Achilles heel seems to be macro viruses, but it also, inexplicably, missed one sample of Avispa.D. It performed particularly well against the Polymorphic test-set, getting all apart from three samples of the Digi.3547 stem and all 500 Cryptor.2582 replicants. This good performance was slightly at the expense of speed.

Look Software Virus ALERT v4.10 3 Feb 1997

ItW Boot	97.8%	ItW File	80.3%
ItW Overall	86.9%	Standard	87.3%
Polymorphic	80.9%	Macro	67.3%

Missing the Moloch and Hare.7750 boot viruses, all the macro samples in the ItW File set and Scitzo *Virus ALERT* turned in a poor performance against the Wild sets. The lack of macro virus detection was a significant factor here, but its problems with Polymorphic and the Standard sets show it has some distance to travel to catch up with the leaders. A stand-alone macro virus product, *Look Virus ALERT for Macros* (available separately) detected 67.3% of the Macro set – generally disappointing.

McAfee VirusScan v3.0.0 15 April 1997

ItW Boot	100.0%	ItW File	99.6%
ItW Overall	99.7%	Standard	98.0%
Polymorphic	90.1%	Macro	99.5%

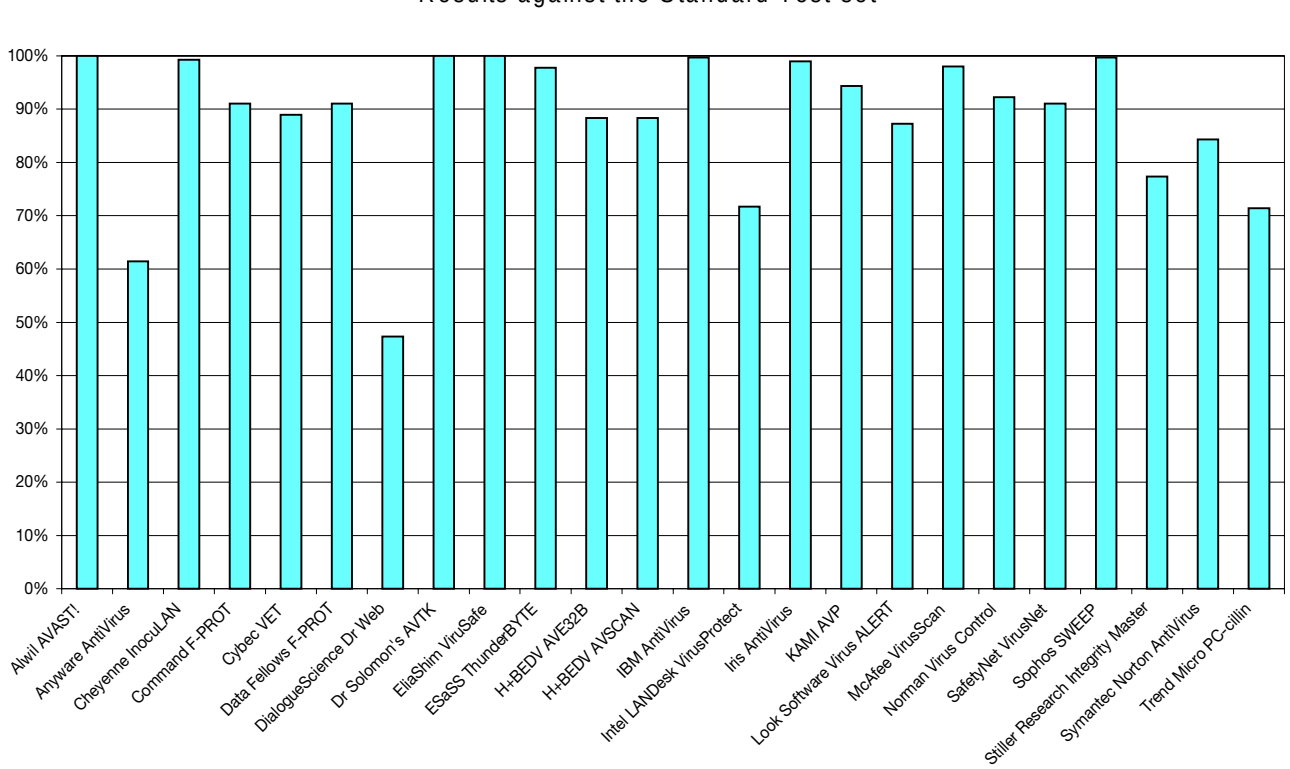
McAfee has obviously been putting in more work on its product, as it has turned in even more impressive results than the last test. It only missed two of the three samples of One_Half.3570 in the wild set, missed Paycheck.A among the macro samples, and of the polymorphics PeaceKeeper.B was missed completely and not all samples of five other stems were found.

The product also showed reasonable speed figures, although no-one will claim that it is the 'Williams of the anti-virus world'. It is good to see such a well-known product turning in results like this in our tests.

Norman Virus Control v4.10 30 April 1997

ItW Boot	100.0%	ItW File	100.0%
ItW Overall	100.0%	Standard	92.2%
Polymorphic	87.4%	Macro	99.1%

As far as the In the Wild set is concerned, this is another perfect performance from this product. It is let down slightly only because in the previous comparative *NVC* registered a 100% score in all categories. It missed three of the four samples of Robocop.A and all four samples of



Nightshade.A in the Macro set, the polymorphs Arianna.3076, Baran.4968 and Cryptor.2582, plus a few samples of Mad.3544, and 25 of the 321 samples in the Standard set.

All that being said, however, it puts in an absolutely perfect performance once again in the area where it really matters for most users – the Wild sets. It also shows a quite acceptable scanning rate. A product that is not only easy to test, but confidence-building.

SafetyNet VirusNet v4.10 April 1997

ItW Boot	100.0%	ItW File	93.7%
ItW Overall	96.1%	Standard	91.0%
Polymorphic	50.3%	Macro	36.5%

VirusNet is a scanner which can be summarized as good at wild and standard viruses, weak on polymorphics and poor at macro virus detection. It detected all of the ItW Boot samples, but missed 36 of the In the Wild File samples – all of these were macro viruses apart from Plagiarist.2051. The product was one of the fastest in the review, but was let down by very poor macro virus detection.

Sophos SWEEP v2.97 May 1997

ItW Boot	100.0%	ItW File	100.0%
ItW Overall	100.0%	Standard	99.7%
Polymorphic	100.0%	Macro	100.0%

An extremely good showing for this package. *SWEEP* was the only product which put in a 100% performance against the Polymorphic test-set.

Scanning speed was a little on the sluggish side; however, if a little more right-foot is at the expense of detection rate, then I for one will be more than happy to see the speed stay the same.

Stiller Research Integrity Master v3.11c March 1997

ItW Boot	92.2%	ItW File	92.3%
ItW Overall	92.3%	Standard	77.4%
Polymorphic	26.4%	Macro	73.7%

Integrity Master is a mark-then-check-later programme, so the main part of the package cannot be evaluated alongside the other scanner products. However, it does have a scanner component, provided for a pre-initialization check – there is no point recording a file's infected state! – and this needs to be reliable in the first instance.

The In the Wild detection rates are reasonable, but anything that does not detect 100% of the Wild set can always be improved. This may be especially important in the role *Integrity Master's* scanner fulfils. It is really let down by its scores against the Polymorphic set. Most samples are missed, and even when some stems are detected, not all of the samples in each were recognized.

Symantec Norton AntiVirus v3.0 1 May 1997

ItW Boot	100.0%	ItW File	97.6%
ItW Overall	98.5%	Standard	84.4%
Polymorphic	83.6%	Macro	94.3%

A slight reduction in detection ability from our last tests, although still acceptable overall. It missed one of the two copies of Desperado.1403, and the single copies of Dir_II.A, Byway.A and Byway.B. Eleven macro samples, and, from the Polymorphic set, all replicants of Arianna.3076, Baran.4968, Cryptor.2582 and Mad.3544 plus two (of 500) samples of Anarchy.6503, were not detected. Finally, the speed is average but acceptable.

Trend PC-cillin v5.04 March 1997

ItW Boot	95.6%	ItW File	98.7%
ItW Overall	97.5%	Standard	71.4%
Polymorphic	80.9%	Macro	73.4%

A slight improvement on the Wild set for *PC-cillin* this time, but at the expense of slightly poorer results against standard and polymorphic samples. It is also weak against the Macro test-set. Four boot samples were missed: Cruel, Hare.7750, Moloch and Neuroquila. Further, ten samples from the Wild set were missed, three of which were *Word* macro viruses; however it also missed Hare.7610 and 7750, HLLC.Even_Beeper.B and Scitzo. The scanner is very slow – the slowest on the test by around six minutes.

In Conclusion…

Comparing these results with those from January suggests that the sizeable increase in the number of macro viruses in the In the Wild File set has taken a toll across the board. No products in this review managed a 'perfect' score as *Norman Virus Control* did in January. However, it is encouraging to see more scanners – five this time – with 100% detection against the In the Wild test-set. Life is not all roses though. Unfortunately, despite excluding *MSAV* from the review, we now find five scanners detecting less than 90% of the total Wild set. Although none of the current batch performed as poorly as *MSAV*, it was the only scanner to score below 90% on the Wild set in January's review. This general fall-off in performance seems to be attributable to the growth in macro viruses and the complexity of adding reliable scanning of OLE files outside *Windows*.

Dr Solomon's AVTK and *Sophos SWEEP* are the apparent picks of this bunch if detection power is your main concern, but don't focus too closely on those near-mystical 100% scores. The *VB* test-set is not 'complete' (more fool those who claim to have one!), thus products that consistently rate over 95% in our reviews should not be overlooked.

VIRUS TEST-SETS

In the Wild Boot Sector test-set. 90 samples of 90 viruses, one each of:

15_Years, AntiCMOS.A, AntiCMOS.B, AntiEXE.A, Boot437, Bootexe.451, Brasil, Bye, Chance.B, Chinese_Fish, Crazy_Boot, Cruel, Da'Boys, Defo, DelCMOS.B, Den_Zuko.2.A, Diablo_Boot, Disk-Killer.1_00, Empire.Int_10B, Empire.Monkey.A, Empire.Monkey.B, Exe_Bug.A, Exe_Bug.C, Exe_Bug.Hooker, FAT_Avenger, FinnishSprayer, Flame, Form.A, Form.C, Form.D, Frankenstein, Galicia, Hare.7750, Ibex, Int40, J&M, Joshi.A, Jumper.A, Jumper.B, Junkie.1027, Kampana.A, Leandro, Michelangelo.A, Moloch, Mongolian_Boot, Music_Bug, Natas.4744, Neuroquila.A, NYB, Ornate, Parity_Boot.A, Parity_Boot.B, Pasta, Paula_Boot, Peter, Qrry, Quandary, Quiver, Quox.A, Ripper, RP, Russian_Flag, Sampo, Satria.A, She_Has, Stealth-Boot.B, Stealth-Boot.C, Stoned-W-Boot, Stoned.16.A, Stoned.Angelina.A, Stoned.Asuza.A, Stoned.Bravo, Stoned.Bunny.A, Stoned.Daniella, Stoned.Dinamo, Stoned.June-4th.A, Stoned.Kiev, Stoned.LZR, Stoned.Manitoba, Stoned.NO_INT_A, Stoned.NOP, Stoned.Spirit, Stoned.Standard.A, Stoned.Swedish-Disaster, Swiss_Boot, Unashamed, Urkel, V-Sign, WelcomB, and WXYC.

Polymorphic test-set. 13,000 samples of 26 viruses, 500 each of:

Alive.4000, Anarchy.6503, Arianna.3076, Baran.4968, Code.3952:VICE.05, Cordobes.3334, Cryptor.2582, Digi.3547, DSCE.Demo, Girafe:TPE, Gripe.1985, Groove_and_Coffeeshop, Mad.3544, MTZ.4510, Natas.4744, Neuroquila.A, Nightfall.4559.B, One_Half.3544, Pathogen:SMEG.0_1, PeaceKeeper.B, Russel.3072.A, SatanBug.5000.A, Sepultura:MtE-Small, SMEG_v0.3, Tequila.A, and Uruguay.

Macro test-set. 722 samples of 182 viruses, made up of:

ABC.A (4), Alien.A (4), Alien.B (4), Alliance.A (4), AntiConcept.A (4), Appder.A (4), Appder.B (4), Atom.A (4), Atom.B (4), Atom.C (4), Atom.D (4), Atom.E (4), Atom.G:De (4), Atom.H (4), Baby.A (1), BadBoy.A (1), BadBoy.B (4), Bandung.A (4), Bandung.G (4), Bandung.H (4), Bandung.I (4), Bandung.N (4), Birthday.A:De (4), Boom.A (4), Boom.B (4), Buero.A:De (4), Cap.A (4), CeeFour.A (4), Chaos.A (4), Clock.A:De (4), Clock.B:De (4), Clock.C:De (4), Clock.D:De (4), Clock.E:De (4), Clock.F:De (4), Colors.A (4), Colors.B (4), Colors.C (1), Colors.D (2), Colors.E (4), Colors.F (4), Colors.H (4), Colors.J (4), Colors.K (4), Colors.M (4), Colors.P (4), Concept.A (4), Concept.AA (4), Concept.B:Fr (4), Concept.C (4), Concept.D (4), Concept.E (4), Concept.F (4), Concept.G (4), Concept.H (4), Concept.J (4), Concept.L (4), Concept.M (4), Concept.W (4), Concept.X (4), Concept.Y (4), Concept.Z (4), CountTen.A (4), Daniel.A (4), Daniel.B (4), Daniel.C (4), Dark.A (4), Date.A (4), Delta.A (3), Dietzel (1), Divina.A (1), Divina.C (4), Divina.E (1), DMV.A (4), DMV.B (4), DMV.C (4), Doggie.A (4), DZT.A (4), Easy.A (4), Friday.A:De (4), Gable.A (4), Gangsterz.A (4), Goldfish.A (4), Hassle.A (4), Hellgate.A (4), Helper.A (4), Hot.A (4), Hybrid.A (4), Hybrid.B (4), Imposter.A (4), Irish.A (4), Irish.B (4), Irish.C (4), Johnny.A1 (4), Johnny.B (4), KillDLL.A (4), Kompu.A (4), Laroux.A (4), Legend.A (4), Lunch.A (4), Lunch.B (4), MadDog.A (4), MadDog.B (4), MDMA.A (4), MDMA.C (4), MDMA.D (4), MDMA.E (4), MDMA.F (4), Minimal.A (4), Minimal.B (4), Minimal.D (4), Muck.A (1), NF.A (4), NiceDay.A (4), NiceDay.B (4), Nightshade.A (4), Nomvir.A:De (4), Nop.A:De (4), Nop.B:De (4), Nop.D:De (4), NPad.A (4), NPad.K (4), NPad.Q (4), NPad.S (4), Nuclear.A (4), Nuclear.B (4), Nuclear.E (4), Outlaw.A (4), Paper.A (4), Paycheck.A (4), Phadera.A (4), Phadera.B (4), Polite.A (4), Rapi.A (4), Rapi.A2 (4), Rapi.B (1), Rapi.G (1), Rapi.H2 (4), Rats.A (4), Rats.B (4), Rats.C (4), Robocop.A (4), Satanic.A (4), Saver.A (4), Sharefun.A (4), ShowOff.A (4), ShowOff.B (4), ShowOff.C (4), ShowOff.G (4), Smiley.A (4), Smiley.B:De (4), Spiral.A (4), Spooky.A:De (4), Stryx.A (4), SwLabs.A (4), Tedious.A (4), Tele.A:De (4), Twister.A (4), TwoLines.A (4), Wazzu.A (4), Wazzu.AF (4), Wazzu.AH (4), Wazzu.AJ (4), Wazzu.AK (4), Wazzu.AL (4), Wazzu.AM (4), Wazzu.AN (4), Wazzu.AO (4), Wazzu.AR (4), Wazzu.AS (4),

VIRUS BULLETIN **©1997 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /97/$0.00+2.50**

Wazzu.AU (4), Wazzu.B (4), Wazzu.C (4), Wazzu.E (4), Wazzu.F (4), Wazzu.H (4), Wazzu.J (4), Wazzu.L (4), Wazzu.O (4), Wazzu.P (4), Wazzu.X (4), Wazzu.Y (4), and Wazzu.Z (4).

In The Wild File test-set. 530 samples of 147 viruses, made up of:

Alfons.1344 (5), Anticad.4096.Mozart (4), Arianna.3375 (4), Avispa.D (2), Backformat.2000.A (1), Bad_Sectors.3428 (5), Barrotes.1303 (6), Barrotes.1310.A (2), BootEXE.451 (3), Burglar.1150.A (3), Byway.A (1), Byway.B (1), Cascade.1701.A (3), Cascade.1704.A (3), Cawber (3), Changsa.A (5), Chaos.1241 (6), Chill (1), Cordobes.3334 (3), CPW.1527 (4), Dark_Avenger.1800.A (3), Delta.1163 (6), DelWin.1759 (3), Desperado.1403.C (2), Die_Hard (2), Digi.3547 (5), Dir_II.A (1), Ear.Leonard.1207 (3), Fairz (6), Fichv.2_1 (3), Flip.2153.A (2), Flip.2343 (6), Freddy_Krueger (3), Frodo.Frodo.A (4), Ginger.2774 (2), Goldbug (3), Green_Caterpillar.1575 (3), Hare.7610 (2), Hare.7750 (8), Hare.7786 (9), Helloween.1376.A (6), Hi.460 (3), Hidenowt (6), HLLC.Even_Beeper.B (3), Istanbul.1349 (6), Jerusalem.1244 (6), Jerusalem.1500 (3), Jerusalem.1808.Standard (2), Jerusalem.Mummy.1364.A (3), Jerusalem.Sunday.A (2), Jerusalem.Zero_Time.Australian.A (3), Jos.1000 (3), Junkie.1027 (1), Kaos4.697 (6), Karnivali.1971 (3), Keypress.1232.A (2), Lemming.2160 (5), Liberty.2857.A (2), Little_Red.1465 (2), MacGyver.2803 (3), Major.1644 (3), Maltese_Amoeba (3), Mange_Tout.1099 (4), Manzon.1414 (2), Markt.1533 (3), Mirea.1788 (2), Natas.4744 (5), Necros.1164 (2), Nightfall.4518.B (2), No_Frills.Dudley (2), No_Frills.No_Frills.843 (2), Nomenklatura.A (6), November_17th.800.A (2), November_17th.855.A (2), NPox.963.A (2), One_Half.3544 (5), One_Half.3570 (3), Ontario.1024 (3), Pathogen:SMEG.0_1 (5), Ph33R.1332 (5), Phx.965 (3), Pieck.4444 (3), Plagiarist.2051 (3), Predator.2448 (2), Prudents.1205.A (1), Quicky.1376 (1), Reverse.948 (3), Sarampo.1371 (6), Sat_Bug.Sat_Bug (2), Sayha (5), Scitzo.1329 (6), Screaming_Fist.II.696 (6), Sibylle (3), Sleep_Walker.1266 (3), SVC.3103.A (2), Tai-Pan.438 (3), Tai-Pan.666 (2), Tanpro.524 (6), Tentacle.10634 (4), Tentacle.1996 (3), Tequila.A (3), Three_Tunes.1784 (6), Trakia.653 (3), Tremor.4000.A (6), Trojector.1463 (6), Trojector.1561 (3), TVPO.3873 (9), Unsnared.814 (3), Vacsina.TP-05.A (2), Vacsina.TP-16.A (1), Vampiro (2), Vienna.648.Reboot.A (3), Vinchuca (3), VLamix (3), Werewolf.1500.B (3), Xeram.1664 (4), Xuxa.1984 (6), Yankee_Doodle.TP-39 (5), Yankee_Doodle.TP-44.A (5), and Yankee_Doodle.XPEH.4928 (2).

…along with the following macro viruses:

Bandung.A (4), Boom.A:De (4), Buero.A:De (4), Colors.A (4), Concept.A (4), Concept.F (4), Concept.J (4), Date.A (4), Divina.A (4), Helper.A (4), Hot.A (4), Hybrid.A (4), Imposter.A (4), Irish.A (4), Laroux (4), MDMA.A (4), MDMA.D (4), NJ-WMDLK1.A (4), NK-WMDLK1.B (4), NOP.A:De (4), NPad.A (4), NPad.D (4), Nuclear.B (4), Rapi.A (4), Wazzu.A (4), Wazzu.C (4), Wazzu.E (4), Wazzu.F (4), Wazzu.J (4), and Wazzu.P (4).

Standard test-set. 774 samples of 321 viruses, made up of:

Abbas.5660 (5), Accept.3773 (5), Account_Avenger.873 (3), Aforia.656 (6), AIDS (1), AIDS-II (1), Aiwed.852 (3), Alabama (1), Alexe.1287 (2), Algerian.1400 (3), Amazon.500 (2), Ambulance (1), Amoeba (2), Anarchy.6503 (5), Andreew.932 (3), Angels.1571 (3), Annihilator.673 (2), Another_World.707 (3), Anston.1960 (5), Anthrax (1), Anti-Pascal (5), Anticad.4096.A (4), AntiGus.1570 (3), Argyle (1), Armagedon.1079.A (1), Assassin.4834 (3), Assignation.426 (3), Attention.A (1), Auspar.990 (3), Autumnal.3072 (6), Baba.276 (3), Baba.356 (2), Backfont.905 (1), Barrotes.840 (3), Beast.498 (2), Bebe.1004 (1), Bell.390 (3), Big_Bang.346 (1), Bill.2658 (5), Billy.836 (3), Black_Monday.1055 (2), BlackAdder.1015 (6), Blood (1), Blue_Nine.925.A (3), Bosnia:TPE.1_4 (5), Burger (3), Burger.405.A (1), Burglar.824 (3), Butterfly.302.A (1), BW.Mayberry.499 (3), BW.Mayberry.604 (6), Cantando.857 (3), Cascade.1701.Jo-Jo.A (1), Cascade.1704.D (3), Casper (1), Catherine.1365 (3), CeCe.1998 (6), CLI&HLT.1345 (6), Cliff.1313 (3), CMOS.3622 (5), Coffeeshop (2), Continua.502.B (3), Cool.929 (3), Cosenza.3205 (2), Cowboy.2487 (2), Coyote.1103 (3), Crazy_Frog.1477 (3), Crazy_Lord.437 (2), Cruncher (2), Cybercide.2299 (3), Danish_Tiny.163.A (1), Danish_Tiny.333.A (1), Dark_Avenger.1449 (2), Dark_Avenger.2100.A (2), Dark_Revenge.1024 (3), Darkstar.439 (1), Datacrime (2), Datacrime_II (2), Datalock.920.A (3), DBF.1046 (2), Dei.1780 (4), Despair.633 (3), Destructor.A (1), Diamond.1024.B (1), Dir.691 (1), Discoloured_Star.223 (1), DOSHunter.483 (1), DotEater.A (1), DR&ET.1710 (3), Ear.405 (3), Eddie-2.651.A (3), Eight_Tunes.1971.A (1), Emhaka.749 (6), Enola_Gay.1883 (4), Entity.1980 (5), F-You.417.A (1), Fax_Free.1536.Topo.A (1), Fellowship (1), Feltan.565 (3), Finnish.357 (2), Fisher.1100 (1), Flash.688.A (1), Four_Seasons.1534 (3), Frodo.3584.A (2), Fumble.867.A (1), Genesis.226 (1), Glacier.1196 (2), Golden_Flowers.1688 (6), Gomer.691 (6), Gotcha.906 (6), Green.1036 (6), Greetings.297 (2), Greets.3000 (3), Halka.1000.b (3), Halloechen.2011.A (3), Hamme.1203 (6), Happy_New_Year.1600.A (1), Hasta.884 (2), HDZZ.566 (3), Helga.666 (2), Helga.666.c (2), Hideos.1028 (6), HLLC.Even_Beeper.A (1), HLLC.Halley (1), HLLP.5000 (5), HLLP.7000 (5), HN.1741 (3), Horsa.1185 (3), Hymn.1865.A (2), Hymn.1962.A (2), Hymn.2144 (2), Hypervisor.3128 (5), Ibqqz.562 (3), Icelandic.848.A (1), Immortal.2185 (2), Inferno.1800 (4), Internal.1381 (1), Intruder.2048 (3), Invisible.2926 (2), Itavir.3443 (1), IVP.1725 (3), Jerusalem.1607 (3), Jerusalem.1808.CT.A (4), Jerusalem.Fu_Manchu.B (2), Jerusalem.PcVrsDs (4), John.1962 (3), Joker (1), Joker.1570 (6), July_13th.1201 (1), June_12th.2660 (6), June8th.1919 (6), June_16th.879 (1), Kamikaze (1), Kela.B.2018 (3), Kemerovo.257.A (1), Keypress.1280 (6), Khizhnjak.556 (3), Kode.145 (3), Korea_Eddy.1316 (6), Korea_Miny.218 (3), Korea_Wanderer.1756 (6), Kranz.255 (3), Kukac.488 (1), Lauren.632 (3), Lavi.1460 (3), Leapfrog.A (1), Leda.820 (3), Lehigh.555.A (1), Liata.327 (3), Liberty.2857.A (5), Liberty.2857.D (2), Liquid_Power.1016 (3), Little_Brother.307 (1), Loren.1387 (2), Lost_Love.853 (6), LoveChild.488 (1), Lutil.591 (3), Maresme.1062 (3), MemLapse.289 (3), Metabolis.1173 (3), Mickie.1100 (3), Midin.765 (2), MonAmi.1085 (3), Monster.424 (3), Mothership.655 (3), MPC.442.c (3), Mummy.1353 (3), Necropolis.1963.A (1), Nina.A (1), November_17th.768.A (2), NRLG.1038 (3), NutCracker.3500.D (5), Odious.569 (3), Omud.512 (1), On_64 (1), Oropax.A (1), Pamyat.2000 (2), Parity.A (1), Paulus.1804 (5), Peanut (1), Perfume.765.A (1), Phantom1 (2), Phoenix.800 (1), Pitch.593 (1), Piter.A (2), Pixel.847.Hello (2), Pizelun (4), Plague.2647 (2), Poison.2436 (1), Pojer.4028 (2), Positron (2), Power_Pump.1 (1), PS-MPC.227 (3), PS-MPC.545 (6), QPA.256 (3), Quark.A (1), Red_Diavolyata.830.A (1), Revenge.1127 (1), Riihi.132 (1), Rmc.1551 (4), Rogue.1208 (6), Rosebud.912 (3), Rubbit.734 (2), Saturday_14th.669.A (1), Screaming_Fist.927 (4), Screen+1.948.A (1), Selfex.1472 (6), Semtex.1000.B (1), Senorita.885 (3), Shake.476.A (1), ShineAway.620 (3), SI.A (1), SillyC.226 (3), SillyCR.303 (3), SillyCR.710 (3), Sofia.43 (3), Soup.1073 (3), Spanz.639 (2), Stardot.789.A (6), Stardot.789.D (2), Steatoda (6), Stud.347 (3), Subliminal (1), Suomi.1008.A (1), Suriv_1.April_1st.A (1), Suriv_2.B (1), Surprise.1318 (1), SVC.1689.A (2), Svin.252 (3), Svir.512 (1), Sylvia.1332.A (1), SysLock.3551.H (2), TenBytes.1451.A (1), Teraz.2717 (5), Terror.1085 (1), Thanksgiving.1253 (1), The_Rat (1), Tigre.1795 (6), Tiny.133 (1), Tiny.134 (1), Tiny.138 (1), Tiny.143 (1), Tiny.154 (1), Tiny.156 (1), Tiny.158 (1), Tiny.159 (1), Tiny.160 (1), Tiny.167 (1), Tiny.198 (1), Todor.1993 (2), Traceback.3066.A (2), Trivial.113 (3), TUQ.453 (1), Untimely.666 (3), V2P6 (1), V2Px.1260 (1), Vacsina.1212 (1), Vacsina.1269 (1), Vacsina.1753 (1), Vacsina.1760 (1), Vacsina.1805 (1), Vacsina.2568 (1), Vacsina.634 (1), Vacsina.700 (2), Vbasic.5120.A (1), VCC.350 (3), Vcomm.637.A (2), VCS1077.M (1), VFSI (1), Victor (1), Vienna.583.A (1), Vienna.623.A (1), Vienna.648.Lisbon.A (1), Vienna.Bua (3), Vienna.Monxla.A (1), Vienna.W-13.507.B (1), Vienna.W-13.534.A (1), Vienna.W-13.600 (3), Virogen.Pinworm (6), Virus-101 (1), Virus-90 (1), Voronezh.1600.A (2), Voronezh.600.A (1), VP (1), Warchild.886 (3), Warrior.1024 (1), Whale (1), Willow.1870 (1), WinVir (1), WW.217.A (1), XWG.1333 (3), Yankee_Doodle.1049 (1), Yankee_Doodle.2756 (1), Yankee_Doodle.2901 (1), Yankee_Doodle.2932 (1), Yankee_Doodle.2981 (1), Yankee_Doodle.2997 (1), Zany.225 (3), Zero_Bug.1536.A (1), and Zherkov.1023.A (1).

PRODUCT REVIEW 1

Dr Solomon's AVTK for Windows 95

Dr Keith Jackson

Dr Solomon's Anti-Virus Toolkit, a name to conjure with. One of the major players in the industry, this product has been around since even before it was the first anti-virus product reviewed by *VB*, way back in the mists of time (July 1989 actually). Since then, the *Anti-Virus Toolkit* (*AVTK*) has been reviewed by VB on three other occasions (June 1991, November 1992, May 1995). This review examines the *AVTK for Windows 95* version 7.70.

Documentation

The product came with three A5 manuals; one each for the DOS and *Windows 95* versions of the software, and a copy of the latest version of the 'Virus Encyclopædia'. These manuals don't seem to have changed overmuch in recent years; indeed, the only change that stands out is that they seem to have been slimmed-down somewhat, and are all the better for that.

As I said in my last review of this product: 'it's very easy to comprehend, reasonably well-indexed, and all in all appears to be a well-balanced effort.' The content of the manuals remains of this high standard – no real complaints at all.

Virus Encyclopædia

The Encyclopædia contains a short description of known viruses, explanations of what a virus can do, and instructions on how to eradicate viruses. The Encyclopædia is available in book form (391 pages), and online (just a click away!).

Judging by the number of index entries, the virus information book contains information on just over 1300 viruses, though as the current version of the *AVTK* claims to detect 11445, the writers of this part of the documentation are obviously struggling to keep up to date. There is a limit, I suppose.

Floppy Problems

The software was provided for review as a set of seven 1.44MB, 3.5-inch floppy disks. Three were for the *Win-dows 95* product, three for the DOS version, and the last was marked 'Magic Bullet'.

I encountered problems reading the *AVTK* floppy disks. The first set I received could not be accessed on my PC: they induced a message saying 'Disk not formatted, would you like to format it now?'. This rather prevented me reviewing anything, so I requested another set of disks. However, this new set solved nothing, exhibiting the same problem.

Donning my Poirot costume, I discovered that the *AVTK* disks could be read by my laptop, and by another desktop PC; therefore, the solution to this problem was to make a copy of each of the floppy disks (yes, all seven), and use these copies for review. This shows that something is on the edge. Probably the floppy drive of my test PC and the copiers used to create *AVTK* disks are at opposite ends of the 'acceptable' spectrum. Has anybody else received floppies from *Dr Solomon's* that they could not read?

Installation

I installed the *AVTK* under *Windows 95*, which proved very straightforward indeed. I merely executed the SETUP program, specified the destination directory, and off it went, merrily copying files. Just over 5MB of hard disk space was used.

When the main bulk of file copying is complete, the user is asked whether the *Windows* memory-resident scanner, WinGuard, and/or the DOS memory-resident scanner, VirusGuard, should be installed. The manual explains that control 'is passed automatically between them as Windows is started up or shut down'. AUTOEXEC.BAT is changed only if the user confirms that this is allowed.

VirusGuard can be set up so that it offers either 'standard security' (executable files are checked during copying and when they are executed), or 'minimum security' (files are checked when they are executed, but files residing on floppy are also scanned during copying). Both security levels scan the diskette boot sector whenever a floppy is accessed. The security level can be changed at a later date if required.

Finally, the user is asked whether the *AVTK* scheduler and/or CLEANBOO (a utility to clean boot sector viruses) should be installed. Installation is now complete, and FindVirus (the scanner component of the product) executes a scan to check that no viruses are present. The next time *Windows 95* is rebooted, the *AVTK* is present and active.

The installation process for this product has always been simple to use, and still is. My previous reviews have stated: 'It's difficult to find any real fault with it' (the installation program). I stand by that judgement.

Operation

The *AVTK* provides easy access to scanning (any available drive), checking (generating and verifying checksums), repair, and looking things up in the Virus Encyclopædia. All these features are readily available by pushing onscreen buttons. Features which can be individually tailored are hidden behind a button marked 'Advanced'. Also available (separately) are the Scheduler, and WinGuard (the memory-resident component).

Dr Solomon's moaned (gently) that in a previous review of the *Anti-Virus Toolkit* I said that the *Windows* version had 'more front than Selfridges'. This is still true; the *Windows 95* version does look very pretty indeed for what is after all merely a utility. It's the way of the world I suppose, that window-dressing (in more than one sense!) is essential to sell anti-virus products nowadays.

Speed

Using the default settings, the *AVTK* scanned the hard drive of my test computer in 21 seconds (whilst checking 715 files). This time increased to 44 seconds when the heuristics option was enabled, and to 61 seconds when all 1395 files were scanned. Finally, the scan time increased enormously to 2 minutes 26 seconds when the option to scan inside ZIP files and PKLITE files was enabled – this is quite a significant difference.

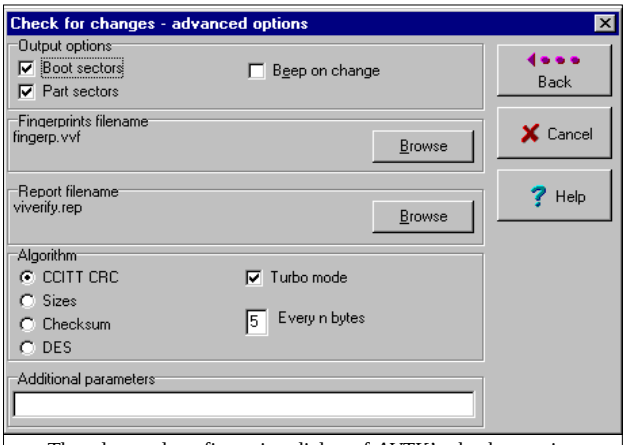
For comparison purposes, the DOS version took 19 seconds to perform the same scan, a time which only increased to 24 seconds when heuristic scanning was enabled. As an independent comparison, *Sophos SWEEP* for DOS took 47 seconds to carry out the same scan.

Scanning

Tested against the Virus Bulletin test-set referred to in the Technical Details section below, the AVTK detected all 476 samples contained in the 'In the Wild' test-set, and all 532 samples of the 'Standard' test-set. 100%; you can't get better than that.

Curiously, when it encountered one of the samples of the Avispa.D virus, the scanner issued a warning message saying 'Please send a sample to Dr Solomon's. This was despite the fact that both samples of Avispa.D were detected correctly, and also despite the fact that the message only applied to one of the two samples.

The *AVTK* even detected all 11,000 polymorphic test samples as infected files, and all 90 of the boot sector samples. One cannot ask for more.



The advanced configuration dialog of *AVTK*'s checksumming component.

AVTK presents this menu when a virus that does not preserve the boot sector is detected.

The log file created by scanning the *VB* test-set contained entries where the virus was 'identified as…', and some where the entry said that 'This virus is like…'.

Heuristic detection can be enabled within the scanner, but given that detection was perfect anyway, it was impossible to test this. However, enabling heuristic detection did add 28 seconds to the time required to scan the CD-ROM containing the *VB* test-set.

I tested the *AVTK* against the *VB* false positive test-set, comprised of 5500 executable files, held on CD-ROM, which have been copied from well-known software products. The *AVTK* checked the entire disk and did not find a single file that it thought was virus-infected, and this stayed the same whether or not the 'Heuristics' option was enabled.

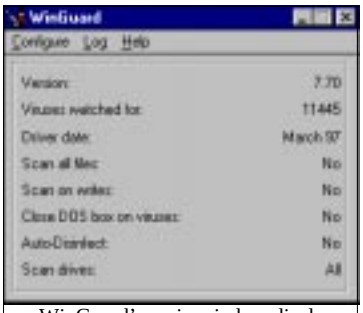
Memory-resident Software

To test the detection abilities of the memory-resident software, I copied the entire virus test from CD-ROM to hard disk, and observed what happened. WinGuard has an option called 'Auto-Disinfect' which can be enabled to allow viruses to be removed from files automatically after detection. The tests described below were performed with Auto-Disinfect active.

Exhaustive testing of WinGuard proved impossible: no matter what I attempted to do, the first time a virus was detected, not only was an error box displayed, but the current action was terminated. I'm not complaining – this is perfectly correct – it just makes it difficult to test things properly. In any case, no matter what I threw at WinGuard manually, it seemed to detect it.

It was possible to test memory-resident virus detection using the DOS program XCOPY. This enabled a set of test samples to be copied from one drive to another, when a special switch setting permitted the selected XCOPY operation to continue even though an error had been detected. Therefore, the only files which were actually copied were those not detected as infected. Given the dual nature of WinGuard and VirusGuard, I suppose this test could be measuring the detection ability of VirusGuard.

The manual is a bit vague as to whether VirusGuard is enabled when a DOS box is entered from *Windows*. It simply says that VirusGuard is 'disabled as Windows is started, and re-enabled when you exit to DOS'. No mention of a DOS box within *Windows*. Make of that what you will. [*According to the developers, WinGuard is active the whole time Windows is running, including inside a DOS box. Ed.*]



WinGuard's main window displays clearly its configuration options.

The log file showed that, during this test, 363 (76%) of the 476 In the Wild samples, and 171 (32%) of the 532 Standard samples had been detected as infected with a virus. These are reasonable results for a DOS memory-resident scanner.

Checksumming

When checksumming is invoked, the user chooses either the DES encryption algorithm, a CCITT CRC, a 'checksum' (mathematics unspecified), or a simple 'file size' test. These methods are listed in order of increasing speed of execution, and decreasing level of security/complexity. The calculated checksums are further secured by the user entering a keyword to seed the checksum calculation process.

These varied options let the user decide whether to trade off increasing checksum security for speed of execution. The user can further speed up checksum calculation by specifying the interval between the bytes included in the checksum calculation (a default of 5 bytes is offered).

I measured the speed of checksum calculation on the hard drive of my test computer using each of the above options. This took 54 seconds when only file sizes were used, 1 minute 3 seconds when 'checksums' were used, 1 minute 45 seconds for the CCITT CRC algorithm, and 3 minutes 4 seconds for the DES algorithm (and this was on a 133MHz Pentium!).

Checksum calculation and verification did not execute at the same speed. Verification was always faster; in some cases much faster. When the above tests were repeated, checksum verification took 15 seconds when only file sizes were checked, 24 seconds when 'checksums' were used, 24 seconds when the CCITT CRC algorithm was used, and 2 minutes 17 seconds when the DES algorithm was used. Note that with the exception of the DES algorithm, all these verification times are *considerably* faster than the corresponding checksum calculation time.

A 'Turbo' option was also available which, when enabled, meant that only the first and last 4KB of each file were checked. However, this option had hardly any measurable effect unless the DES algorithm was used.

These measurements were all made with the 'Turbo' option active, but when it was disabled, the checksum generation time with the DES algorithm in use rose to 14 minutes 21 seconds, and the verification time rose to 13 minutes 45 seconds. Only someone with time on his hands would use the DES algorithm to calculate checksums without the 'Turbo' option active.

The Rest

Included with the *AVTK* is a single floppy disk entitled the 'Magic Bullet'. This floppy disk contains a bootable system that can be used when a 'known clean' DOS disk is not available. This is an excellent idea, which works well, but the README file cautions that problems may be encountered when the Magic Bullet is used with a hard disk which uses multiple partitions.

Both the *AVTK* scheduler and the program CLEANBOO (that cleans boot sectors) seem to work well. I've nothing much to say about either of them.

Conclusions

Even since the early days of *VB*, *Dr Solomon's Anti-Virus Toolkit* has always been shown to be very good at detecting viruses. The above results confirm that this still holds true today in its *Windows 95* incarnation.

Purely Windows versions of anti-virus software raise nagging doubts about viruses bypassing some of the checks. After all, it is not possible to boot *Windows 95* systems entirely from 'known clean' floppy disks – it's too large, and files stored on the hard disk must inevitably be used. The developers of the *AVTK* obviously think the same way, as the DOS version of the product is provided in the *Windows 95* pack. However, the world has moved on, and *Windows 95* anti-virus programs are what sell, so that's what Dr Solomon's provides. Simple really.

If you want a *Windows 95* scanner, you will not go far wrong purchasing this product. There are products around which are as good at detecting viruses, but not very many that are better.

Technical Details

Product: *Dr Solomon's Anti-Virus Toolkit v7.70*.

Developer/Vendor: *Dr Solomon's Software Ltd*, Alton House, Gatehouse Way, Aylesbury, Buckinghamshire HP19 3XU, UK. Tel +44 1296 318700, fax +44 1296 318734, email support@drsolomon.com, WWW http://www.drsolomon.com/.

Availability: Any PC running *Windows 95* with at least 5MB of free hard disk space.

UK Prices: £80 for one copy of the full single- user product. Corporate and site licensing prices should be discussed with a *Dr Solomon's* sales representative.

Hardware used: A 133MHz Pentium with 16MB of RAM, a 3.5-inch floppy disk drive, a CD-ROM drive, and a 1.2GB hard disk divided into drive C (315MB), and drive D (965MB). This PC can be configured to operate under *Windows 95*, *Windows 3.11*, *Windows 3.1*, or DOS 6.22.

Viruses used for testing purposes: Listings for the Standard, the In the Wild File, and the Polymorphic test-sets can be found in *VB*, March 1997, p.17. Details of the In the Wild Boot sector test-set are in *VB*, June 1997, p.23. Where more than one variant of a virus is available, the number of examples of each virus is shown in brackets after the virus name (if the total is greater than one). For a complete explanation of each virus, and the nomenclature used, please refer to the lists of PC viruses published regularly in *VB*.

PRODUCT REVIEW 2

AVP for NetWare v3.0

Martyn Perry

After a series of *Windows NT* products, this month we return to *NetWare*, to take a look at *AntiVirus Toolkit Pro for NetWare* (*AVPN*) from *Kami Associates*.

The product is licensed on a per-server basis with a sliding scale of discounts depending on the total number of servers licensed. The product is shipped with a key file, AVP.KEY, which is needed to run the application, and which contains the licence information. In the evaluation set, this file already had the company details and key code pre-loaded. No separate workstation software is shipped – workstations would use a separate product such as *AVP* for DOS or Windows to provide client support.

Presentation and Installation

The evaluation product was shipped as a single ZIP file, without documentation. The archive unpacked into three directories: 3_XX, 4_XX and INTRANET. Each directory provided the necessary files for 3.xx, 4.xx and Intranet versions of *NetWare*. Installation to the server is effected by copying the files from the directory appropriate to the target installation (in this case 3.xx) to a server directory – the default is SYS:AVPN.

Once the *AVPN* files have been copied to the server, a *NetWare* NCF file needs to be created to load the various NLMs. It must be tailored for the specific version of *NetWare*, but a typical example is SYS:AVPN\AVP_3x.NCF, which contains:

```
search add sys:avpn
load sys:avpn\avpnut.nlm
load sys:avpn\avp3f.nlm
load sys:avpn\avp30.nlm -q1200
```

This loads AVPNUT.NLM, and AVP3.NLM or AVP3F.NLM depending on the version of CLIB on the server. The final line loads AVP30.NLM, the main program. It is important to include the command option '-q1200', which sets the queue size for the online scan.

Loading the Program

When the main NLM program is loaded, the user is presented with the main administration screen. The program adopts the same menu format as other *NetWare* utilities.

The scanner provides for immediate, online (real-time), and timed scans. An immediate scan allows the user to start and stop the scan on command from the server console. The screen displays the progress of the scan with the display of the files checked and any viruses found. An online scan allows scanning either when a file is copied to or from the server or when a file is accessed on the server, and a timed scan uses the immediate settings on a scheduled basis.

The scanner administration is performed only at the server console. The main menu gives options to set configuration, view current configuration, begin scan, view report, and reload base. Online help is available by pressing F1 in the appropriate menu.

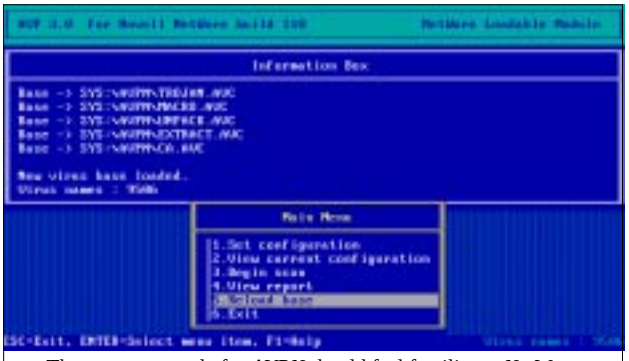
Configuration Options

Scanner options are configured under Set Configuration. Those provided include the time interval between scheduled scans (which can be set to monthly, weekly, daily, or repeated every n minutes), message options, and scan options (including file types).

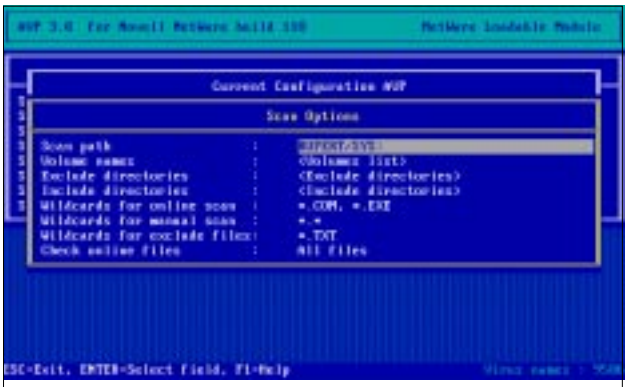
The message options define what alarm message text is issued in the event of a virus being detected. The default is 'Virus detected'. Under this option comes user names (defining a list of users who will be recipients of any message), and send to pager – if this option is set to yes, AVPN stores the alarm message in AVPALARM.TXT, in the same directory as the program files. This option is slightly misleading, in that an external pager program is required to broadcast the pager message, and will have to be configured, since AVPN does not include integrated pager support.

Under scan options, the scan path setting provides the initial directory for a manual scan – SERVER/SYS is the default: if an entry is made here, it is displayed when an immediate scan is started as the default path to scan. The volume names provide a list of volumes for online and automatic scanning. Specified directories can also be excluded or included, to customize the scanning list.

Also under scan options are settings for the file extensions to be scanned. These can include wild card characters, and there are separate settings for online scanning (the defaults



The system console for *AVPN* should feel familiar to *NetWare* administrators.



The set configuration menu also uses typical *NetWare* console controls.

are *.COM, *.EXE), and for manual scanning (the default is *.*). There is also an option specifying files to exclude from all scans (the default is *.TXT).

The final option in this section selects the type of files which will be checked: none, new files, existing files, or all files – the default is all files. Here, 'new files' equates to incoming files to the server. Similarly, 'existing files' includes outgoing files, and those opened for view/edit.

AVPN allows for packed files to be unpacked and their contents scanned, and for archive files to be decompressed and their contents scanned. It checks not only for known viruses, but may also use a heuristic analysis option. These options can be set to 'on' for files to be scanned in neither, either, or both manual and online scans.

Further file options include the making of a backup copy or moving infected files to a designated directory before attempting disinfection.

In the case of infected files, various actions are available: none (no action, report only), disinfect (attempt to clean the infection), delete (erase file), remove (move infected file to a designated directory – the default AVPN\VIR), and rename (rename the file with the extension .VIR).

AVPN integrates with client-end scanners (*AVP* for DOS or *Windows*). Thus, when one of the *AVP* clients is run on a workstation logged in to a *NetWare* server which is running *AVPN*, the client scanner can report any infections to the server-based scanner.

The product offers four actions to take should a virus infection be detected on an attached workstation: none (no action), send message (warn user), and message with logout (warn the user and disconnect the workstation from the network). A further option, remote password, is displayed, but not implemented in this release.

Two directory options can be defined; one for 'removed' files, which acts as the destination directory for files moved with the remove option, and a directory for temporary files, which acts as a location to store temporary files created when unpacking archives, etc.

Log Files and Other Options

AVPN uses one log file, which stores the information in a file in the program directory (AVP.LOG is the default file name). The size of this file can be limited if required.

The user may choose from the following options which messages are to be reported: infected files, suspicious files, warnings, packed files, archived files, and clean files. Date- and time-stamps can also be added to the messages. Further, the online and manual scans can be selected independently for reporting.

The option 'view the current configuration' shows the current settings. 'Start the scan' begins an immediate scan of the selected areas. The default path, specified under the scan path options, is displayed. This can be amended, if required, and the scan can be stopped from the console.

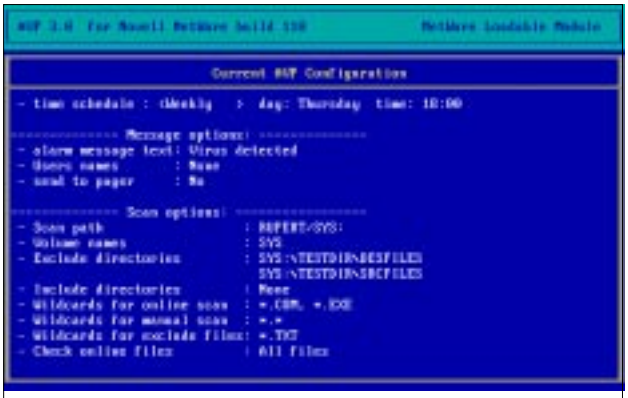
The view report option displays the contents of the file AVP.LOG; however, there is no specific facility to produce a printed copy.

Alert Management and Updates

AVPN handles alerting of infections in several ways: a message is sent to the server console during the scan, a pager message can be created in the program directory in the file AVPALARM.TXT, the offending user can be logged out of the network, or a predefined group of users can be notified.

To update the product, it is necessary simply to replace the various signature files (.AVC) and update the AVP.SET file, which contains a list of the signature files which need to be present. The AVC files in the test-set are: CA, EXTRACT, KERNEL, MACRO, TROJAN, UNPACK, and AVP9703.

Updates are effected by copying the new files to the program directory and using the Reload base option on the main menu. This saves having to close the application and reload the NLMs whenever a new virus signature database is installed.



The configuration options you would expect in a server-based scanner…

Detection Rates and Overhead

The scanner was checked using the usual three test-sets; In the Wild, Standard and Polymorphic (see the summary table for details). The virus signature list used, AVP9703, claimed knowledge of 9506 virus strains.

Undetected viruses were identified by using the 'move infected files' option and listing all the files which remained in the virus directories. The tests were conducted using the default scanner file extensions. The default list was all files, excluding those with a TXT extension.

AVP's score against the In the Wild set was near perfect, only missing one file – Avispa.D. Against the Standard test-set, however, 87 samples were missed, and in the Polymorphic set, *AVPN* failed to detect the whole Arianna.3375 stem.

To determine the impact of the scanner on the server performance, we timed how long it took to copy 63 EXE files (4,641,722 bytes) from the SYS:PUBLIC from one server directory to another using *Novell's* NCOPY. Using NCOPY keeps the data transfer within the server itself and minimizes network effects.

The directories used for the source and target were excluded from the virus scans to avoid the risk of a file being scanned while waiting to be copied. Because of the different processes which occur within the server, these time tests were run ten times for each setting and an average calculated (see the summary for detailed results). The tests were:

- NLM not loaded: establishes the baseline time for copying the files
- NLM unloaded: run after the other tests to check how well the server is returned to its former state
- NLM loaded; no scan active: tests the impact of the scanner loaded in its quiescent state with no real-time or immediate scan in progress
- NLM loaded; scan new files only: shows the impact of running the real-time scan on incoming files without the immediate scan
- NLM loaded; scan existing files only: shows the real-time scan effect on outgoing files
- NLM loaded; scan all files: shows the real-time scan effect on incoming and outgoing files
- NLM loaded; scan all files, and immediate scan active: shows the incremental effect of running the immediate as well as the real-time scan

The initial impact of loading the scanner software is minimal; however, the impact of the scanner becomes apparent when a real-time scan is started. Interestingly, the additional overhead of running the on-demand scanner is minimal. The residual overhead, when *AVPN* is unloaded is slight, and due to the AVP3F, CLIB, and STREAMS NLMs remaining on the server.

Conclusion

After reviewing a number of Windows NT products, the style of the console screen on a NetWare-based product now appears dated. Having said that, the product provides the necessary functionality required of a server product, apart from the lack of multi-server support.

The detection rate was good, and the incremental overhead when running the immediate scanner was remarkably low. The one item to consider is the queue size. If this is insufficient, the online scan could be compromised. In all, *AVPN* is a good performing scanner with an extensive range of configuration options.

AntiVirus Toolkit Pro for NetWare v3.0

Detection Results

Test-set[1]	Viruses Detected	Score
In the Wild File	508/509	99.8%
Standard	678/765	88.6%
Polymorphic	11500/12000	95.8%

Overhead of On-access Scanning:

The tests show the time (in seconds) taken to copy 63 EXE files (4.6MB). Each test is performed ten times, and an average is taken.

	Time	Overhead
Program not loaded	6.9	–
Program unloaded	7.0	1.4%
NLM Loaded (all options set to 'no' unless otherwise stated)		
Scan no files	7.1	2.9%
Scan new files only	14.8	115.8%
Scan existing files only	16.5	141.2%
Scan all files	16.9	146.3%
Scan all files; immediate scan	17.0	147.6%

Technical Details

Product: *AntiVirus Toolkit Pro for NetWare, v3.0*.

Developer/Vendor: *KAMI Ltd*, 10 Geroev Panfilovtcev St, 123362 Moscow, Russia. Tel +7 095 948 4331, fax +7 095 913 5087, email sales@avp.ru.

Distributor US: *Central Command Inc*, PO Box 856, Brunswick, Ohio 44212, USA. Tel +1 330 273 2820, fax +1 330 220 4129, email sales@command-hq.com.

Price: All prices in US dollars, including monthly updates for one year. Single-server licence: $299.95; 2–5: $995.00; 6–10: $1790.00; 11–25: $3975.00; 26–50: $6950.00; 51–100: $10,900.00; 101–150: $13,550.00. For pricing on larger licences, contact the company.

Hardware Used:

Server – *Compaq Prolinea 590*; 80MB RAM with a 2GB hard disk, running *NetWare 3.12*.

Workstation – *Compaq 386/20e*, 4MB RAM with a 207MB hard disk, running DOS 6.22 and *Windows 3.1*.

[1]**Test-sets:** For a complete listing of all the viruses used, see *VB*, May 1997, p.20.

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, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, England

Tel 01235 555139, International Tel +44 1235 555139
Fax 01235 531889, International Fax +44 1235 531889
Email: editorial@virusbtn.com
World Wide Web: http://www.virusbtn.com/

US subscriptions only:

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

Tel +1 203 431 8720, fax +1 203 431 8165

END NOTES AND NEWS

The *MIS Training Institute* is sponsoring a **conference on *Audit and Security of Intranets*** from 18–20 August 1997, in Surrey, England. Amongst many others, such topics as intranet management challenges, viruses and Trojan horses, and firewalls will be addressed. For further details, contact Patricia Fischer on Tel +44 171 779 8292, fax +44 171 779 8293.

***Sophos Plc's* next round of anti-virus workshops** will be on 9/10 July 1997 at the training suite in Abingdon, UK. The company's training team is also hosting a *Practical NetWare Security* course on 3 July 1997 (cost £325 + VAT). Another initiative sees the company throwing open its doors to any organization wishing to evaluate anti-virus software. The move is aimed at helping administrators of multi-server networks to see how they can best implement virus protection within their organization. Information is available from Karen Richardson, Tel +44 1235 544028, fax +44 1235 559935, or access the company's World Wide Web page; http://www.sophos.com/.

The **24th Annual Computer Security Conference and Exhibition** will be held in Washington DC from 17–19 November 1997. This event features over 120 sessions covering such topics as Network Security, Encryption, and Product Issues. Information can be found on the *CSI's* Web site; http://www.gocsi.com/.

Dr Solomon's Software Ltd (formerly *S&S International*) is presenting **Live Virus Workshops** in the UK on 15/16 July 1997; details from Melanie Swaffield at *Dr Solomon's*. The company has also launched a new anti-virus software package for *Lotus Domino*. The product is said to scan automatically all inbound and outbound email messages, isolating any files detected as infected. For details of this and the company's other products, Tel +44 1296 318700, or visit the *Dr Solomon* Web site at http://www.drsolomon.com/.

The **Fourth Annual Computer Security Audit and Control Conference** (COSAC) will be held from September 15–18 in Newcastle, County Down, Northern Ireland. For a conference brochure and booking details, contact Helen Hawkins on +44 1232 738080, or email helen@akaassociates.demon.co.uk.

British-based *Calluna Technology Ltd* has launched a hardware product which it says is the first 'to offer a fully comprehensive security solution for the Internet and PCs'. The card is described as an **intelligent hardware virus isolator and anti-hacking devic**e, and is claimed to provide total protection against such threats as virus infection and data corruption. For details, contact Tamara O'Connor or Helen Dinsdale of the *A Plus Group*; Tel +44 1753 790700, or email connor@aplus.co.uk or hdinsdal@aplus.co.uk.

The UK government IT certification body, *ITSEC*, has unveiled a revamped Web site. Now to be found there are online versions of the UK certified product list, a searchable archive of press materials, and a range of information on the scheme. **Visit the ITSEC Web site at http://www.itsec.org.uk/**.

***CompSec 97* will be held in London** from 5–7 November 1997. The conference aims to help highlight the risk to IT systems, assess security shortcomings, and protect against fraud, disaster, and negligence. Information is available from Amy Richardson at *Elsevier Science*; Tel +44 1865 843643, fax +44 1865 843958, or email a.richardson@elsevier.co.uk.

Free virus checking is now available on the Internet by connecting to house-call.antivirus.com, reports *Computerworld*. The service is provided by *Trend Micro*, and uses an ActiveX component, which downloads to the user's machine, to scan for, and remove, common viruses [*Dangerously interesting… Ed.*].