*ISSN 0956-9979* *FEBRUARY 1998*

# VIRUS BULLETIN

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

## *IN THIS ISSUE:*

• **Uno, DOS, tres…** This issue's comparative review tests eighteen products for DOS. Which products were given a VB 100% award this month? Keep up with the latest, starting on p.12.

• **White Knight?** *IBM's* Dave Chess has a long history in the anti-virus industry. Catch up with him in the Insight column on p.6.

• **Big Business:** We reveal how one of the UK's largest corporations handles a virus outbreak. Read about the *AA's* anti-virus procedures on p.8.

## CONTENTS

# EDITORIAL

## Start Spreading the Word

The other day I was pondering what, if anything, interesting happened in the virus field in 1997. We saw macro viruses roughly double in number between January and June and again between June and December. In fact, this was something of a slowdown in the growth rate. Since Concept's appearance, their numbers have been doubling approximately every two to three months. The macro virus problem has mushroomed following the initial discovery of what is now known as WM/Concept.A around August 1995 to about 2000 identified, named families and variants today.

Still, reaching the first thousand macro virus mark in less than two years of the rise of a new class of virus shows there is something 'special' about macro viruses, or maybe *Word* macro viruses in particular. The rate of spread and increase in number is clearly *not* what was implied by *Microsoft's* rather euphemistic name for Concept – 'the Word Prank Macro'. So why have they taken off?

> *“ hitching a new virus to a* Word *document… is quite an inspired move ”*

It is generally agreed that two or three factors account for the rise in number of macro viruses and macro virus incidents. The first is that versions six and seven of *Microsoft Word* (those initially capable of supporting complex macro viruses), were common, or became common soon after Concept's release. Thus, there was a large installed base of infectable machines. Secondly, macro viruses are easy to write, especially if you have one or two as a 'guide' and have installed all of the WordBasic documentation *Microsoft* helpfully included with *Word 7*. Combined, these factors mean that an easy-to-use, widely-available 'development environment' exists. This largely accounts for the rapid increase in numbers.

However, there are probably around 15,000 to 16,000 families and variants of program infectors – why do they still only account for a very small portion of virus incident reports? They are certainly numerous enough!

The usual answer to this question is that numbers alone are not very important. Akin to motive alone not being sufficient to convict a murderer, opportunity is necessary to see a virus become widespread. To this end, boot viruses have something of an advantage – traditionally, diskettes are exchanged much more than program files, neatly accounting for the widely observed fact that although they only comprise about 10% of viruses, boot infectors accounted for over 50% of virus incidents (pre-Concept, that is). Targeting such a popular word-processor, macro viruses have enjoyed an advantage similar to that of boot viruses, in that *Word* document files are widely, and relatively freely, shared. There is another string to the macro virus bow, however. Email.

The release of *Windows 95*, with its bundled *MS-Mail* client, saw many more PC users start using *Word* and *MS-Mail* together, as an email client. Many users still habitually exchange 'email' without the vaguest notion that they are actually sending *Word* documents around as attachments. This is largely what has made the difference between the early prevalence of other kinds of viruses and the growth in reports of macro viruses. This is hardly a revelation.

However, 1997 saw the development of two new viruses which suggest that authors of file infectors may be becoming interested in improving the spread of their creations. Anarchy.6093 (*VB*, October 1997, p.6) and Navrhar (*VB*, November 1997, p.15) both directly manipulate *Word* document files to 'inject' macros that drop the virus. Aside from the technical challenge of 'infecting' documents without using the *Word* environment, this suggests the authors of these viruses were interested in bettering their creations' chances. In Anarchy's case, this seems to have worked.

Dropping a virus from a *Word* document, *per se*, is hardly new – Nuclear was clearly trying to do it back in late 1995 (*VB*, November 1995, p.8). Deliberately hitching a new virus to *Word* documents however, would seem to be a new twist on this idea. As *Word* documents are the fastest (current) method of global code transportation, this seems (in one sense) to be quite an inspired move.

I suspect we will see this 'trick' employed more often in 1998.

# NEWS

## Anybody Out There?

Sarah Gordon, virus researcher at *IBM's T J Watson Center* in New York, and a member of *VB's* Advisory Board, is appealing for first-hand experiences of non-virus malicious software attacks. A brief questionnaire about the specific nature of the attack, its impact on the company concerned and its PCs will be forwarded to anyone answering the call for information.

While full contact details are required, they will be treated in the strictest confidence. Please contact:

Sarah Gordon
T J Watson Research Center
PO Box 704
Yorktown Heights
New York 10598
USA

Voicemail: +1 914 7847388
Fax: +1 914 784 6054

Work email: sgordon@watson.ibm.com
Alternative email: sgordon@dockmaster2.ncsc.mil ▮

## Gotcha!

*Integralis Technology Ltd* claims in a recent survey that 75% of all organizations are failing to enforce IT security policies. The survey targeted sixty companies each with a minimum of five hundred email users. Well over half of these companies have Web-enabled desktops, and allow their staff personal use of email.

*Integralis'* survey underscores the dangers faced by businesses which are giving employees greater access to the Internet, while omitting to implement company-wide security policies. Specific threats include junk mail, hidden viruses, JAVA and ActiveX applets, as well as confidentiality and liability issues.

The results are reminiscent of those found in a survey sponsored by *Symantec* as featured in the July 1997 *Virus Bulletin*. In that user poll, it was discovered that, despite the availability of monthly software updates, more than 50% of users did not bother to implement them ▮

## VB'98: Call for Papers

It is that time of year again, when thoughts at *Virus Bulletin* turn towards conference planning. To that end, we are now seeking submissions for inclusion in the programme. Abstracts of about 200 words must reach *VB* by Friday 27 February 1998. Please send your submissions to Conference Manager Alie Hothersall (fax +44 1235 531889 or email alie@virusbtn.com) ▮

### Prevalence Table – December 1997

| Virus | Type | Incidents | Reports |
|---|---|---|---|
| CAP | Macro | 93 | 20.8% |
| Concept | Macro | 27 | 6.0% |
| Parity_Boot | Boot | 22 | 4.9% |
| Wazzu | Macro | 21 | 4.7% |
| AntiEXE | Boot | 20 | 4.5% |
| Form | Boot | 19 | 4.3% |
| Laroux | Macro | 19 | 4.3% |
| Npad | Macro | 18 | 4.0% |
| Empire.Monkey | Boot | 15 | 3.4% |
| Ripper | Boot | 15 | 3.4% |
| Junkie | Multipartite | 9 | 2.0% |
| Temple | Macro | 9 | 2.0% |
| Dodgy | Boot | 8 | 1.8% |
| Kompu | Macro | 8 | 1.8% |
| NYB | Boot | 7 | 1.6% |
| Sampo | Boot | 7 | 1.6% |
| Appder | Macro | 6 | 1.3% |
| Edwin | File | 6 | 1.3% |
| Monkey | Boot | 6 | 1.3% |
| DelCMOS | Boot | 5 | 1.1% |
| MDMA | Macro | 5 | 1.1% |
| Natas | Multipartite | 5 | 1.1% |
| ABCD | Boot | 4 | 0.9% |
| Imposter | Macro | 4 | 0.9% |
| Showoff | Macro | 4 | 0.9% |
| Bandung | Macro | 3 | 0.7% |
| EXEbug | Multipartite | 3 | 0.7% |
| Niknat | Macro | 3 | 0.7% |
| Rhubarb.215 | File | 3 | 0.7% |
| Schumann | Macro | 3 | 0.7% |
| Spanska.4250 | File | 3 | 0.7% |
| WelcomB | Boot | 3 | 0.7% |
| Others [1] | | 64 | 14.3% |
| Total | | 447 | 100% |

[1] The Prevalence Table includes two reports each of: AntiCMOS, Baboon, Die_Hard.4000, Galicia.800, Influenza, Jerusalem.1367, LBB_Stealth, Maverick.2048, One_Half.3544, Stoned.Angelina, Switcher and Tequila; and a single report of each of Aardvark.307, ABC, Amberman.438, Anxiety, Burglar.1365, Bye, Cascade.1661, Cascade.1701, Chance.B, CountTen, Cruel, Datalock.920, DZT, Eater.2167, Ebcav.378, Europe_'92.421, Goldfish, HLLO.9999, HLLP.16474, Inexist, Istanbul.1349, Jakarta.559, Jumper.B, Kampana.A, Maniak, Maverick.1536, NiceDay, Quandary, Rapi, RP, Russian_Flag, Sack, Safwan, SheHas, Skim.1455, Swlabs, Urkel.B, V2PX.1236, V-sign and Werewolf.1450.

# 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 January 1998. 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 | **M** | Infects Master Boot Sector (Track 0, Head 0, Sector 1) |
| **D** | Infects DOS Boot Sector (logical sector 0 on disk) | **N** | Not memory-resident |
| **E** | Infects EXE files | **P** | Companion virus |
| **L** | Link virus | **R** | Memory-resident after infection |

**Coconut.1870**

**CN:** An encrypted, appending, 1870-byte direct infector, infecting two files at a time. It contains the text ‘[by @King Lizard]’. Infected files have the word 4E49h (‘IN’) at offset 0003h. On 25 and 31 December, the virus displays an ‘ASCII-art’ smiley face image with a Christmas message.

```
Coconut.1870        E8EA FF3E 83BE 4D08 013E FF8E 4D08 720A AD2B C133 C1D3 C0AB
```

**Delta.1128**

**CER:** An encrypted, stealth, 1128-byte appender containing the texts ‘Your Cmos is gone. Good bytes from (DEL)ta Virus !!! Reset in 30 seconds !’ and ‘Brazil - 02/96’. The payload, which triggers on 29 November, changes the CMOS data, effectively disabling the disk drives.

```
Delta.1128          1F0E 07BE 2300 03F5 8BFE B95D 043E 8A66 04FC AC32 C4AA E2FA
```

**DSA.263**

**CR:** An appending, 263-byte virus containing the text ‘[DSA by Rajaat / Genesis]’. Infected files start with the word 4B50h (‘PK’).

```
DSA.263             A301 0150 B401 C0E4 06B9 0701 BA00 01CD 21B8 0042 33C9 99CD
```

**Eddy.1386**

**CER:** A stealth, prepending, 1386-byte virus. Infected files have their time-stamps set to 58 seconds. The following template also covers a 1551-byte variant.

```
Eddy.1386           B0FF B40F 86E0 90CD 213D 0101 7504 E83C 0090 B821 3590 CD21
```

**Friend.301**

**PN:** A companion, 301-byte virus infecting one file at a time and containing the texts ‘[Friend] The first Corean Companion virus..(c) 1997/09 Osiris of CVC (Corean Virus Club),Corea’ and ‘COM*.EXE’.

```
Friend.301          B43C B903 00BA A002 CD21 93B4 40B9 2D01 BA00 01CD 21B4 3ECD
```

**Gisela.702**

**CR:** An appending, 702-byte virus containing the text ‘c:\command.com’. On 21 January the virus displays the usually encrypted message ‘Virus GISELA 2.0 By EJECUTOR (Hecho en Argentina) Feliz cumpleaños Gisela.’ Infected files have the string ‘GI2’ at the end of code.

```
Gisela.702          891E A500 8C06 A700 6825 2158 86C4 BA20 01CD 21B8 004B 0410
```

**Hal**

**MDR:** A one-sector boot sector virus infecting MBR on a hard disk and DOS Boot sector on a floppy. It contains the plain-text signature ‘HAL 3001’ at offset 00F1h. During a boot from an infected disk, a user has 1 in 8 chances of seeing this text displayed.

```
Hal                 BB00 048B 4713 33FF 33F6 4889 4713 505B B105 FEC1 D3E3 5307
```

**Hunter.253**

**CN:** An encrypted, overwriting, 253-byte direct infector containing the texts ‘Hunter 2’, ‘MAD MAN’ and ‘[SLAM]’. Infected files have the byte EAh at offset 0003h.

```
Hunter.253          BB41 0166 A00A 013C 0074 0C66 3007 4302 C781 FBE4 017E F4C3
```

**Hunter.324**

**CN:** An encrypted, overwriting, 324-byte direct infector containing the texts ‘Hunter’, ‘MAD MAN’ and ‘[SLAM]’. Infected files have the byte EAh at offset 0003h.

```
Hunter.324          BB46 0166 A00A 013C 0074 0C66 3007 4302 C781 FB2D 027E F4C3
```

**IVP.673**

**CEN:** An encrypted, appending, 673-byte, fast, direct infector containing the texts ‘ShOck -[IvP]- Dark Warrior [IVP]’, ‘*.com’ and ‘*.exe’.

```
IVP.673             8D9E 1801 B973 022E 8AB6 A303 2E8A 2732 E62E 8827 43E2 F5C3
```

**Leon.1194**

**CER:** An encrypted, 1194-byte appender containing the text ‘(c) Leonard. Constanta, Romania.’

```
Leon.1194           8ED9 5683 C672 908B FE4E B937 04D9 D0FC AC32 042A C2AA E2F8
```

**MM.786**

**ER:** An appending, 786-byte virus containing the encrypted texts ‘The MEHRGAN virus dosn’t destroy data, Don’t panic.’ and ‘Only for Thanking from MEHRGAN MAHDAVY.’ The virus’ ‘Are you there?’ call, INT 21h AX=4B57h (‘QK’), returns the value AX=5653h (‘SV’).

```
MM.786              3D51 4B75 05B8 5356 9DCF 80FC 4B74 2780 FC56 7422 80FC 4374;
```

**MrR.962**

**CR:** An encrypted, appending, 962-byte virus containing the texts ‘COMMAND.COM’ and ‘MrRAVEL - Carmen.’. Infected files have the word 724Dh (‘Mr’) at offset 0003h.

```
MrR.962             582D 0300 95BF AB03 03FD 2E81 3DC3 C374 16B9 9603 BF2C 0003
```

**MrR.983**

**CR:** An encrypted, appending, 983-byte virus containing the texts ‘COMMAND.COM’ and ‘MrRAVEL - BOLERO.’. Infected files have the word 724Dh (‘Mr’) at offset 0003h.

```
MrR.983             582D 0300 95BF C003 03FD 2E81 3DC3 C374 16B9 AB03 BF2C 0003
```

**MrR.1000B**

**CR:** An encrypted, appending, 1000-byte virus containing the texts ‘COMMAND.COM’ and ‘MrDivide Overflow.’. Infected files have the word 724Dh (‘Mr’) at offset 0003h.

```
MrR.1000B           0300 9095 BFC1 0303 FD90 2E81 3DC3 C374 18B9 BA03 90BF 2E00
```

**MrR.1000C**

**CR:** An encrypted, appending 1000-byte virus containing the texts ‘COMMAND.COM’, ‘MrRAVEL - Carmen.’ and ‘BUCURESTI 1994.’. Infected files have the word 724Dh (‘Mr’) at offset 0003h.

```
MrR.1000C           582D 0300 95BF C103 03FD 2E81 3DC3 C374 16B9 BC03 BF2C 0003
```

**MrR.1294**

**CR:** An encrypted, appending, 1294-byte viruds containing the texts ‘COMMAND.COM’, ‘SSdivide overflow’ and ‘CHKDSK.EXESCANDISK.EXENDD.EXE’. Infected files have the word 5353h (‘SS’) at offset 0003h.

```
MrR.1294            9F50 BFCD 0403 FD51 2E81 3DC3 C374 16B9 E604 BF28 0003 FDB2
```

**Rogue.1807**

**CER:** An encrypted, appending (COM) and prepending (EXE), 1807-byte virus containing the texts ‘EXECOM’, ‘MS-DOS cheking MCB’s.’, ‘Please wait...’, ‘ I’am The Rogue. ’, ‘*.CPS’, ‘*.*’ and ‘C:\C.*’. All files executed while the virus is active, have their time-stamps set to 60 or 62 seconds.

```
Rogue.1807          068B F70E 1F8C C3B4 ??1E 07B9 F006 90FC AC32 C4AA FEC4 E2F8
```

**Sarcoma.1328**

**CER:** A stealth, 1328-byte appender containing the texts ‘ ‘COMPUSARCOMA’ virus  by M.S.S.’, ‘C:\CONFIG.SYS’, ‘C:\COMMAND.COM’ and ‘SHELL’. The virus adds 100 years to the date-stamp of infected files.

```
Sarcoma.1328        E800 005E 83EE 0AB8 5757 CD21 3C75 7467 1E8C D848 8ED8 8A16
```

**Taek.1638**

**CER:** An encrypted, 1638-byte appender containing the text ‘Welcome to Blue Scorpion Virus. Copyright (C) 1995-1996 Taek Software. All rights reserved.’. Infected files have their time-stamps set to 58 seconds.

```
Taek.1638           BE?? ??B9 3506 2E8A 0434 ??2E 8804 46E2 F5??
```

**TPVO.539**

**EN:** An appending, 539-byte direct infector containing the texts ‘*.EXE’ and ‘  This is Super Harlem! virus by Harlem Liangof[TPVO] in Keelung, Taiwan <R.O.C>’. Infected files have the word 4453h (‘SD’) at offset 0012h.

```
TPVO.539            B440 B91B 028D 9400 01CD 21B8 0042 33C9 33D2 CD21 B440 B918
```

**Trivial.186**

**CN:** An appending, 186-byte, direct infector containing the text ‘*.COM’. Infected files have the byte 2Ah (‘*’) at offset 0003h.

```
Trivial.186         2D03 0089 84AE 01B4 408D 9400 01B9 BA00 90CD 10B8 0042 33C9
```

**Tupac.1308**

**CR:** An appending, 1308-byte virus containing the text ‘The Tupac Amaru virus, dedicated to all the people of the MRTA who were killed by Fujimori’s troops after surrendering at the japanese embassy on Lima, to all the people killed and tortured in his government, and finally to all those who work for democracy and for a better world. Wintermute/29A’. The virus contains some anti-debugging tricks.

```
Tupac.1308          B8A9 25CD 210E 1FB8 0135 CD21 3E8C 860F 053E 899E 0D05 8D96
```

**Ufo.1501**

**ER:** An encrypted, 1501-byte appender containing the texts ‘UFO’, ‘THEY... are here ! We will see who is gonna survive, motherfuckers ! You are all some fuckin Unknown Flying Objects ! UFO has come to destroy the fucking thresh around here !’ and ‘UFO message : I am sick of a bullshit like you, motherfucker ...’. On 5 May, 6 September and 1 October, it corrupts the CMOS data.

```
Ufo.1501            BB03 00B9 2201 2EA0 0600 2630 0743 E2FA BB50 01B9 8D04 2630
```

**Ugra.1394**

**ER:** A polymorphic, appending, 1394-byte virus, avoids infecting files with names ending with ‘AN’, ‘IT’, ‘AV’, ‘OT’ and ‘RU’. The virus contains a few destructive payloads like destroying the CMOS data, overwriting sectors on the hard disk, turning the hard disk into the Idle state (using direct disk access method). The following template can be used to detect the virus in memory only.

```
Ugra.1394           268B 3E6C 0489 3F4B 4B31 3F01 3FE2 F8BB 9605 BEE9 0432 ED32
```

**Ultimate.419**

**CN:** A polymorphic, appending, 419-byte, direct, fast infector containing the texts ‘Evil’, ‘*.COM’ and ‘Ultimate Evil by Evil One’. Infected files have the plain-text string ‘Evil’ at offset 0010h. It is impossible to detect the virus using a simple template.

**UndyingLover.708**

**CR:** An encrypted, appending, 708-byte virus, containing the text ‘[UnDyinG LoVeR v2.0c][by WârßläDÉ/DÇ ’96]’. The virus payload overwrites the DOS Boot Sector of the default partition. Infected files have their time-stamps set to 58 seconds.

```
UndyingLover.708    3E8B 96B2 028D B612 0052 50B8 0533 CD21 585A B940 01EB 1490
```

**V.667**

**ER:** An appending, 667-byte virus containing the text ‘C:\WINDOWS\SYSTEM\KRNL386.EXE’. The virus sets the attribute of this file to Hidden. Infected files have the word FEDCh at offset 000Ch.

```
V.667               BA56 02CD 21B8 DCFE CD21 81F9 DADA 744F 0633 C08E D8C4 3E84
```

**WPCB.3207**

**CER:** A partially encrypted 3207-byte appender containing the texts ‘SVH] - LIPA’, ‘I will always loves you !’ and ‘-o-  Take a bunch of care  -o-’. Time-stamps of infected files are set to 62 seconds.

```
WPCB.3207           AC32 0588 4600 2630 4702 83EB 044C 81FC 4C01 7404 0BDB 74D8
```

# INSIGHT

## Chess Piece

Dave Chess has come a long way since his first ‘real job’, one summer at the chemical research facility where his father worked. He put that early ‘taste for research and oddly-smelling corridors’ to such good effect at *IBM* during the summer vacations which followed, that the company hired him full-time, fresh out of college in 1981.

Currently, he is working for Steve White at the *Watson Research Center* in a group known variously as IBM AntiVirus R&D, Massively Distributed Systems and the High Integrity Computing Lab. As usual, there is a lot on his plate – ‘We do IBM AntiVirus, of course, as well as research on the Immune System for Cyberspace. I also work on security issues in mobile code systems, keep an eye on emergent (i.e. non-traditional) security aspects of Java and ActiveX, *Lotus Notes* and that sort of thing, and generally mess about.’

Dave is one of the original anti-virus ‘good guys’. His interest in computer viruses started when they did in 1987, and his recollection of the first panicky reports shows how he became personally involved from the start. ‘At first I thought it was just media hype, but then it occurred to me that a virus might get into *my* system, and mess with *my* files. So, I wrote a tiny, simple modification-detector and made it available inside *IBM*. I also started talking to Steve White and Bill Arnold, who were interested in computer security stuff also. The rest is history!’

### The Past

Born in a Chicago suburb, Dave moved to New York state with his family when he was five years old, and has lived there ever since. He graduated Summa Cum Laude from Princeton with a BA in Philosophy in 1981, and married his college sweetheart two years later. Both received Master of Science Degrees in Computer Science from Pace University after enrolling in night classes. Asked if his training in Philosophy had any relevance to the battle against viruses, he says ‘I think it does, although not directly. Studying Philosophy trains you to analyse problems, to get to the heart of debates, to think about thinking. If nothing else, I can often see two people in the heat of debate, and figure out just where they really agree and disagree’.

One of his first positions at *IBM* was that of a ‘Help Desk person’. Having released its first PC – ‘a rather silly idea, I thought at the time’ – *IBM* recruited Dave as a ‘Consultant’, a contact point for users with problems and faults to report. At that time, his experience in the field of personal computers was limited to the creations his father, an amateur radio operator, had made. Dave remembers ‘fiddling with a little Motorola Microprocessor Kit he had put together down in the hamshack (sixteen buttons and four 7-segment LEDS, programmed in machine code; it was great fun!)’.

He is typically modest about his progress, recalling how he soon became Manager of the PC Consulting Group – ‘that is, the PC Help Desk!’ – at *Watson Research*. It was then that his old preference for research and hands-on development led to a new role in the company. ‘After a year, I decided I liked technical stuff better than management. For several years I ran *IBM’s* internal conferencing disk (BBS, computer conference) about the *IBM* PC family, and did miscellaneous programming.’

In his position as PC consultant he had witnessed the advent of troublesome PC viruses and he very soon became hooked, ‘Lehigh and CHRISTMA were the first viruses I actually looked at, followed shortly by Vienna.648 and Jerusalem. My first virus experiences were pretty much all of the form – “I think I might have a virus, and so-and-so tells me that you’re the guy to talk to”.’

Asked for his most memorable virus support incidents, Dave mentions many sessions on the telephone, helping users ‘infected with Monkey.B who had used FDISK /MBR on bad advice’, usually from a friend. The individual incidents, he recalls, ‘blur together – talking people through DEBUG is hard work, but hearing how pleased they are when all that mumbo-jumbo they’ve been typing causes their files to reappear is a nice reward…’.

The ‘National City Corporation incident’ also sticks in Dave’s memory as a great success story. ‘We were able to get into what was a very urgent situation and give them what they needed much faster than they expected. It’s always nice when everything comes together perfectly! Of course, as we automate everything it will be the machines doing most of the work, and we won’t even realize what a good job we’re doing!’, he says with a grin.

### The Present

Years on, he is still regarded as a virus authority. As anti-virus technology grows ever more sophisticated in response to more complex viruses, it is not surprising that Dave is working on the development of *IBM’s* automatic ‘virus immune system’. He believes that the immune system strategy should become standard in the corporate world in the near future.

‘Users should certainly know a few common-sense things, like not running programs from strangers, but on the whole virus defenses should be automatic and nearly invisible… that means that little or no user interaction should be required on the infected workstation to detect and repair an incoming infected object.’

While he works on the ideal, he advocates pragmatism in the face of reality: ‘Whatever works, I want to use. Static heuristics, for instance, turn out to work quite well on boot records and macro viruses; on the other hand no-one’s figured out how to do it well on binary files. Either false positive or false negative results (or both!) come out unacceptably high. So I like static heuristics where they work, and I don’t like them where they don’t.’ What if someone beats him to a virus panacea? Dave is characteristically open-minded and humorous about the prospect, vowing, ‘If someone were to actually figure out how to Detect All Known and Unknown Viruses tomorrow, without making machines unusable in the process, I would welcome the new method with open arms.’

Despite its early prominence in the virus and anti-virus explosion, Dave no longer sees America as significantly different from the rest of the world, or at least the rest of the West. He appreciates that the Internet has freed many fields from the bounds of geography, and that anti-virus research is definitely one of them. The linguistic and cultural barriers that are instrumental in slowing down both virus and anti-virus spread in Russia, Asia and South America are coming down too. ‘Certainly, many of the people I work with every day are outside the US; in many cases I may not know (or care) where in the world they are.’

Stressing the importance of the big picture, he refers to the relatively young anti-virus field as the ‘obscure step-child’ of computer security, and is a firm believer in the benefits of a closer relationship between the two.

Dave is not laying any bets on the direction the anti-virus industry is taking into the 21st century. ‘I think it’s clear’, he points out, ‘that the best solutions in the future will be those that are tied in the best, both to the customer’s overall computing and security setup, and to a globally-distributed anti-virus system. But the details are hard to predict; it’s important to stay aware and active, and able to innovate quickly to deal with the world as it changes.’

In an effort to further this aim, he has collaborated with colleagues at the *Watson Research Center* on a couple of papers in the area of the security of mobile code (agents, active content and the like). ‘A bunch of us here wrote a paper called “Mobile Agents: are they a good idea?” quite a while back (I worked mostly on the security section).’ This has become a very heavily-cited paper in this emerging field, and recently Dave was responsible for updating it for reprinting in a book on the subject, published late last year. He has also written the introductory/overview paper of a forthcoming book which focuses specifically on mobile agent security. Both texts are part of *Springer-Verlag’s* ‘Lecture Notes in Computer Science’ series and Dave is understandably proud of them, ‘they have an impact on the broader world, outside the anti-virus corner.’

When pressed, he accuses virus writers of ‘behaving irresponsibly and immorally, and often illegally’. Unlike many of his colleagues, and in line with other researchers like Sarah Gordon, he does have a degree of sympathy for them. ‘We certainly need, as a society, to understand them, both because it will help us understand how to motivate them to behave more responsibly, and because as fellow humans we have an obligation to try to understand them as well as we can.’ Despite his current hopes for the *IBM Immune System* development program, he is realistic about times to come, admitting that ‘the virus problem, and variations on it, will be with us for some time.’

His abiding interest in all things technical sees him keeping an eye on the development of *IBM’s* chess-playing computer –‘Deep Blue is way cool, both because it plays such good chess, and because it makes us think about what it means to be intelligent, to think, to be human.’

So, does he follow his namesake game? ‘I’m the rawest of woodpushers: I know the moves, but don’t really seem to have the patience for the combinations and the deeper strategies. On the other hand, I love the *culture* of chess, and I devour every chess book I can find that isn’t just a long series of game transcripts and combination problems.’

## The Future

The Chess household in Mohegan Lake, New York is often crowded. Dave and his wife Margaret, daughter Mayanne, and son Elias share their home with adopted stray cats Star and Stripe, and assorted mice and hamsters. When he is able to, Dave likes to walk in the mountains or bake bread to relax. Even in his quieter moments, he is hungry for information – ‘In what little time the job and the kids leave me for hobbies, I tend to sit in a large, soft chair and read. Mainly science-fiction novels, mystery novels, short stories of just about any kind, *Wired* and *Scientific American* and *World Press Review*.’

We asked Dave if he was aware that he had something of a reputation as a fast speaker. ‘Oh, yeah! When I see myself on videotape, I have to get Margaret to translate for me. She can understand what I’m saying, but I can’t. Whenever I give a talk, I warn the audience first that I tend to speak much too fast, and if I start doing it today they should wave their arms in the air. I’ve got much better at it in talks, but person-to-person I still wax incomprehensible frequently.’ [*Future* VB *conference attendees, take note! Ed.*]

Living up to his name, Dave Chess is the most strategic of game players. Thanks to his early association with the computer security industry, he is also something of a paradox – a highly technical researcher with first-hand experience of ‘tech support’, and a cautious realist cherishing a notion of a virus-free world!

FEATURE

# The Fourth Emergency Service Protects Itself

*John Butler and Mark O’Connor*
*Automobile Association, UK*

The *Automobile Association* (*AA*) was established in 1905 to protect and promote motoring. Today, the *AA* attends nearly five million vehicle breakdowns a year. It is the UK’s largest motoring organization.

Information technology, in which the *AA* invests more than £1 million a week, is the organization’s lifeblood. It has thousands of PCs, hundreds of *NetWare* servers, several mainframes, and *Oracle* and *Ingres* databases running on Unix servers.

With most of these resources networked nationwide, utilizing many outside contractors, and making increasing use of the Internet in daily operations, security and data integrity are major concerns. To address the threat posed by viruses, the *AA* has a comprehensive computer security programme, which includes virus prevention and detection capabilities.

## Background

Anti-virus detection and eradication procedures were implemented company-wide in 1991. Over time, the anti-virus procedure manual became impractical, due to its length, and was increasingly awkward to keep up to date. Ensuring widespread distribution of the latest version became harder, while possible infection sources, such as the Internet and diskettes from other organizations, increased in number and complexity.

A flow chart was conceived to overcome these problems. We present it here as an informal depiction of the *AA’s* anti-virus procedure. A certain amount of common sense must be applied to its interpretation, otherwise some branches could be infinite loops. The actual chart is reproduced on a laminated A3 sheet, allowing quick and simple distribution to all relevant parties within the *AA*. The chart provides staff and contractors with an easily-assimilable overview of the appropriate course of action in the event of an alert from their anti-virus software.

The *AA* has chosen two anti-virus products to protect desktop PCs, and servers, respectively. *Dr Solomon’s AVTK* is deployed on all high-risk PCs and was chosen for its high detection and very low false alarm rates. *Intel LANDesk Virus Protect* was chosen for the *NetWare* servers and lower-risk PCs because of its advanced logging, reporting and infection alerting mechanisms. Together these products meet the organization’s requirements.

## The Process

To understand the process, start at the top of the flow chart. The *AA* Service Desk is the central location to which all suspected faults are reported. Those classified as ‘priority one’ are handled by Problem Management. Viruses rate as the highest priority, meaning that the problem should be resolved within an hour.

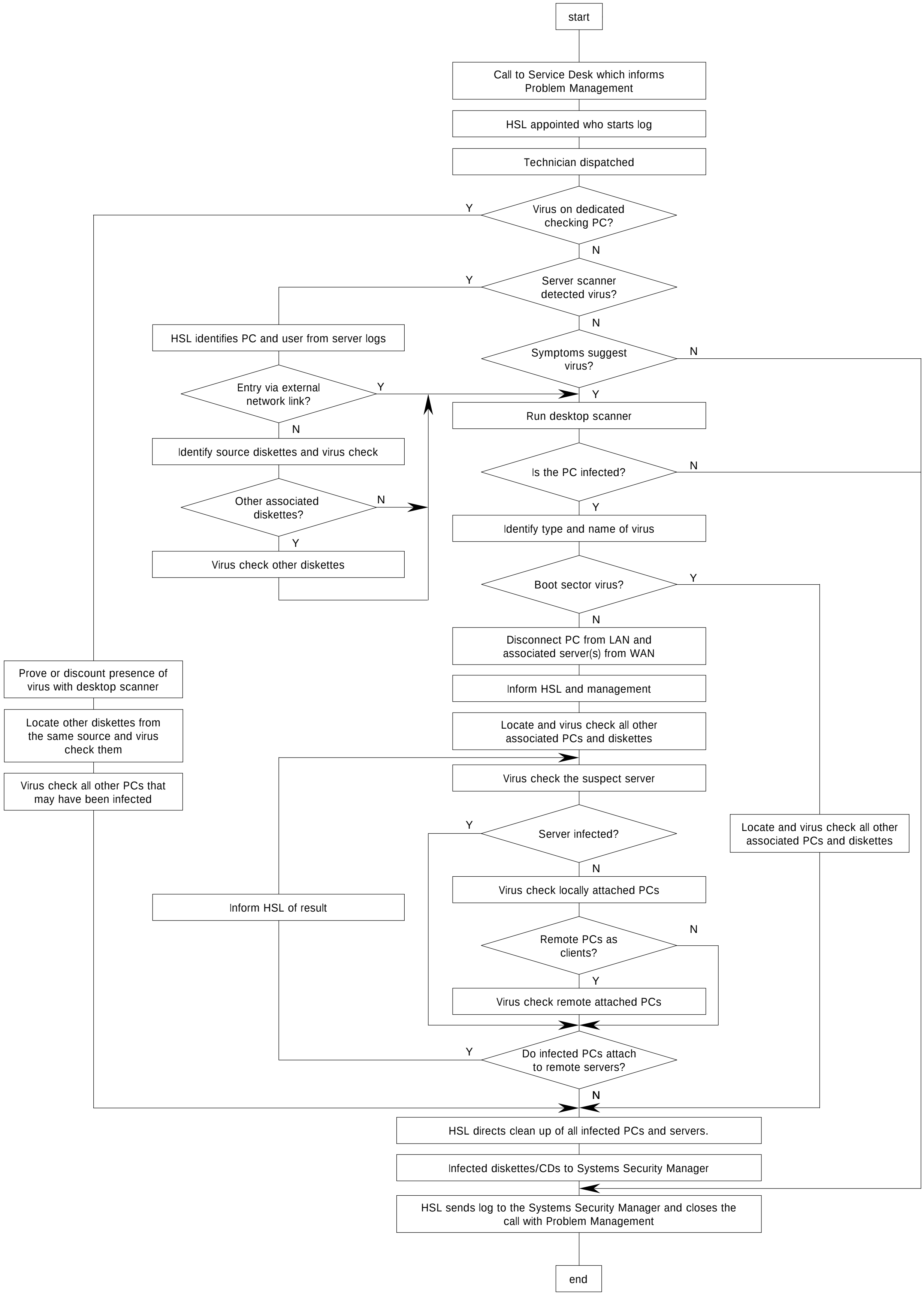
When a suspected virus is reported, a specially trained Hit Squad Leader (HSL) is selected to coordinate the response. Once the original symptoms have been described, the HSL decides on a course of action and starts a log, which forms the basis of the final report. At this stage, one of the *AA’s* fifty IT technicians is dispatched to carry out an on-site investigation, informing the HSL of their progress. Depending upon the source of the original report, the response may differ in the following ways.

There are more than thirty standalone, dedicated virus-checking PCs situated in all major *AA* locations. These are used to check all incoming disks and CD-ROMs, with the approved desktop scanner. Suspect files may have to be sent to the anti-virus vendor for positive identification. However, if a virus is confirmed by the scanner, the technician or HSL checks the source of the diskette to determine if infected media have entered at other locations. Further to this, the technician must check PCs that may have used infected media. If this is the case, a separate procedure is instigated at the Service Desk.

Another source of the original report may be the server-based scanner. On detection of a virus, a warning is issued to all the users logged into that server. This scanner’s logs provide the network address of the PC on which the virus was found, together with the username associated with the client logon. If the virus originated from an external modem connection or through the firewall from the Internet, this indicates a file virus, which carries the highest risk of rapid network infection. If it originated on a diskette, other disks from the same source must also be checked.

The final source of reports is from *AA* staff describing symptoms displayed by their PCs that may be virus-related. A suspect PC is checked with the approved desktop scanner, and if the PC is not infected, the call is closed.

If the PC *is* infected, it is important that the virus is positively identified by name and type. If the virus is a boot sector infector, all potentially infected PCs and diskettes must be traced and scanned. In the case of a file virus, the infected PC is also isolated from the LAN immediately and, as a precaution, the server is disconnected from the WAN. There are no exceptions to this rule, which ensures maximum security while allowing local users to continue their work. At this point, Problem Management is notified so as


start
Call to Service Desk which informs Problem Management
HSL appointed who starts log
Technician dispatched
Virus on dedicated checking PC?
Y
N
Server scanner detected virus?
Y
N
HSL identifies PC and user from server logs
Symptoms suggest virus?
N
Entry via external network link?
Y
Y
Run desktop scanner
N
Identify source diskettes and virus check
Is the PC infected?
N
Other associated diskettes?
N
Y
Identify type and name of virus
Y
Virus check other diskettes
Boot sector virus?
Y
N
Disconnect PC from LAN and associated server(s) from WAN
Prove or discount presence of virus with desktop scanner
Inform HSL and management
Locate other diskettes from the same source and virus check them
Locate and virus check all other associated PCs and diskettes
Virus check the suspect server
Virus check all other PCs that may have been infected
Locate and virus check all other associated PCs and diskettes
Y
Server infected?
N
Virus check locally attached PCs
Inform HSL of result
Remote PCs as clients?
N
Y
Virus check remote attached PCs
Y
Do infected PCs attach to remote servers?
N
HSL directs clean up of all infected PCs and servers.
Infected diskettes/CDs to Systems Security Manager
HSL sends log to the Systems Security Manager and closes the call with Problem Management
end

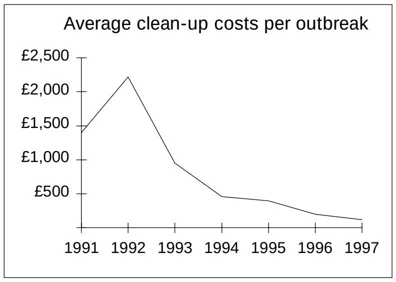
to deal with service calls arising from the disconnection. The technician, meanwhile, informs the HSL so that the priorities of the Business Department may be settled with local line management. All other potentially infected PCs and diskettes must be traced and tested. If further viruses are found, another procedure is initiated.

If the infection has spread to the local fileserver, all attached PCs must be virus checked. It must also be established whether any of them attach to remote servers, and if they do, those servers are checked in turn. The HSL informs the owners of potentially infected machines, and gives the go-ahead to clean PCs and servers.

Prior to this, all evidence of file date- and time-stamps must have been collated. This may provide forensic evidence when investigating the origins of an outbreak. Where necessary, all affected files are replaced from clean master copies or backups. The IT Security Department uses the diskettes for further investigation and as possible police evidence. They may also be needed for evidence to give to the originator of the virus. The log is sent to IT Security and the call closed with Problem Management.

### Summary

Over the years the *AA's* virus protection, detection and eradication procedures have been refined and improved, leading to reduced clean-up costs within the organization. The flow chart eases the users' interpretation of steps to follow after a virus alert. With an imminent move to *Word 8* (most users currently have *Word 2*), it will be interesting to see what procedural changes, if any, may be required.



# VIRUS ANALYSIS

## Creepy Crawly

*Oleg Petrovsky*
*Cybec Pty Ltd*

RustyBug.5330 appears to belong to the generic family of high level language (HLL) viruses. Its body is compressed with LzExe, or an LzExe-compatible utility. The virus prepends itself to host files, or more precisely, replaces the first 5330 bytes with its code before attaching the original part to the end. The relocated section is encrypted to make disinfection more difficult.

This virus is a fast, direct infector. It propagates very quickly by infecting COM and EXE files – searching for potential victims through both the current subdirectory and the subdirectories listed in the PATH statement. RustyBug identifies EXE programs by checking for the initial 'MZ' signature. As a result, RustyBug will infect not only DOS executables, but also other programs such as NE, PE or LE format executables.

### Executing an Infected Program

When an infected program is run, execution starts with the decompression engine attached by the LzExe compression utility. Once loaded in memory and unpacked, the virus' code grows to 35K, consisting of the decompressed executable code and a vast number of empty data fields reserved as static buffers. After decompression, the virus looks for the checksum files of some popular integrity checkers – specifically ANTI-VIR.DAT, CHKLIST.MS, and CHKLIST.CPS. If any of these are found, they are deleted. RustyBug makes sure that target files have their attributes correctly re-set before trying to delete them. By this crude method, the virus attempts to protect itself from detection by system integrity checkers. Deleting database files certainly prevents the affected programs from locating modified files. On the other hand, such acts of vandalism should attract the attention of watchdogs, looking for the first sign of trouble. Unfortunately, some integrity checking utilities will simply recreate the database if the old one cannot be located.

RustyBug takes no chances – it tries to delete database files after every new, successful infection. Needless to say, the infection process is both slow and easy to spot because of the 'unnatural' disk activity. The virus code resides in memory in its unpacked form. It does not attempt to recompress itself during infection (perhaps too much to expect from someone trying to 'impress the world' with a couple of lines in HLL put together into a trivial DOS infector). Opting for an easier solution, RustyBug performs yet another disk access and re-reads the packed version of the virus from the currently executed file, preserving it in memory for future use.

Then, the virus organizes a new Disk Transfer Area and assigns it to its own PSP:0080 address, before proceeding through the main infection loop. Finally, when the infection procedure is complete, RustyBug executes the original host program. Once again, the virus author opted for an easier but more time-consuming and conspicuous method of programming. It appears to have been too difficult to reconstruct the original EXE file and make it ready to execute. The virus re-reads the original file, decrypts the last 5330 bytes and writes them back to the beginning of the program. This means that the virus disinfects the host on disk so the DOS EXEC function (Int 21h AH=4Bh) can load and execute it. When control is passed back to the virus code, RustyBug reinfects the program it cleaned just a moment earlier. A few more disk access calls later, the virus finishes its long shift and retires.

### The Main Infection Loop

There are no hidden surprises here, just the standard find first/find next scenario of spreading infection. First the virus processes all ‘MZ’ files in the current directory, stepping through every COM file. It checks potential targets for an existing infection. Clean files are infected and closed. It then deletes all the integrity database files, lowering its chances of detection. The virus looks for targets in sub-directories listed in the PATH statement and stored in the environment segment, going through the same routine every time. It propagates fairly quickly, especially through the DOS and *Windows* directories commonly in the PATH.

### Infecting Files

On finding a potential host, RustyBug first checks its size. It will not infect anything shorter than 5330 bytes – the size of the virus itself when compressed. The original date and time-stamp are preserved. The virus then reads four bytes from the offset 001Ch. If the file is already infected, the two-word sequence 0F9Eh, 9C93h will be found there. If the file is clean, the virus reads 5330 bytes from the start of the file, encrypts them, and attaches them to the end. Then it places the packed version of the virus at the start. This way RustyBug takes control when the infected file is run.

### Encrypting Algorithm

The virus uses a straightforward XOR instruction together with a more convoluted algorithm, to encrypt the 5330-byte block of the original file. The encryption key changes with each successive byte, starting with the initial value of 1Bh. Every second byte is encrypted with the key, and after moving to the next byte, the key is incremented by one. When the value of the key reaches FFh, it is changed to 0Eh. The next chunk is now encrypted, starting with the key value of 0Eh, incrementing the key by one and the address by two. When the key reaches FFh, it is changed to 0Fh, which becomes the initial key for the next chunk.

This means that every chunk is encrypted with a different initial key (block I - 1Bh, block II - 0Eh, block III - 0Fh, block IV - 10h etc) using the same algorithm (key +1, address +2, until the key = FFh). This continues until a chunk of 5330 bytes is encrypted. Since the encryption scheme is reversible, the decryption algorithm is identical. Using a simple C-like notation we can show the encrypting/ decrypting process:

```
Initial_Key = 1Bh
for (key = Initial_Key; key = < FFh;)
{
  encrypted = original XOR key
  key = key + 1
}
Initial_Key = 0Eh
Until all 5330-byte block is processed
{
  for (key = Initial_Key; key = < FFh;)
  {
    encrypted = original XOR key
    key = key + 1
  }
  Initial_Key = Initial_Key + 1
}
```

Apart from being irritating during the infection process, RustyBug does not appear to have any destructive payloads. Randomly (with about a 1 in 200 chance), the virus displays a moving star-field similar to the effect implemented in one of the Spanska viruses. The image, in graphic mode, shows white dots of varying intensity and speed, moving from the right to left of the screen. The animation disappears after a key is pressed.

### Bugs Encountered

The virus corrupts programs that use a DOS extender to switch into protected mode, as it cannot handle the execution of such files. If the infected program is a PE or NE and executed within *Windows*, the virus activates and runs the original code, but is incapable of reinfecting it, leaving the program clean. Fortunately, bugs inside the find first/find next loop stop the virus infecting every single suitable host, thus slowing down propagation.

### Conclusion

The RustyBug virus has found its way into the wild; this is not due to its clever design or the specific talents of its author, but rather, in spite of them. Its fast spread can be accounted for by the sheer volume of files the virus tries to infect in one go. What is more, the files RustyBug finds in directories specified in the PATH, are always those most frequently used.

## RustyBug.5330

| | |
|---|---|
| Aliases: | HLL.5330, HLLP.5330. |
| Type: | COM, EXE file direct infector. |
| Self-recognition in Files: | |
| | 0F9Eh, 9C93h at offset 001Ch. |
| Hex Pattern in COM and EXE Files: | |
| | 8B05 5F5A D981 009D B9FD 36D0<br>4F0C 4DE8 9B05 0FEB E020 CEDC |
| Trigger: | One in two hundred chance on infected program execution. |
| Payload: | A graphic mode star-field animation will be displayed. |
| Removal: | Under clean system conditions, restore infected files from backup or replace with originals. |

# COMPARATIVE REVIEW

## What's up, DOS?

The last *Virus Bulletin* DOS comparative was in July 1997. Of the eighteen products up for testing this time around, sixteen of them featured in that last review. The two newcomers this month are both Eastern European – *AVG* from the Czech company *Grisoft*, and *NOD-iCE* from the Slovak Republic's *ESET*. This is also the first *VB* review to feature the revamped *Data Fellows F-Secure Anti-Virus*.

As with other recent *VB* DOS comparatives, the focus of this review is on detection rate and speed. This review does introduce a change, however. Over the last few years, *VB* has run DOS comparatives approximately six-monthly, but this is the only such comparative for 1998. With the Win32 platforms (*Windows 95* and *NT*) firmly in the ascendancy, and their increasing importance throughout the business and personal computing sectors, we have decided to focus our attention more on these platforms, providing two comparatives for each, every year.

There were no limitations on the software we asked the vendors to submit, other than that they had to run as DOS applications. Some developers still ship a separate macro virus scanning program with their 'normal' scanner as the only (or most reliable) way of detecting these increasingly important viruses

Including separate scanning components can be seen as a positive or a negative thing. Whilst a macro-only scanner could be a useful option in some circumstances, most computer users seem to want a complete anti-virus solution. Reflecting this, we tested the most appropriate component of multi-scanner packages against each test-set. As the In the Wild File set contains both parasitic executable infectors and macro viruses, this means that some otherwise good packages cannot score a 'perfect' 100%. These products are thus precluded from attaining the coveted VB 100% award through a design decision.

### The Tests

The speed tests in this review were carried out on a Pentium machine with 64 MB of RAM. When speed was not an issue, a variety of other machines were also used – the aim being to produce the results in a reasonable period of time by sheer weight of numbers.

For the detection test, the virus test-sets were stored in a read-only directory on a *NetWare* server and the samples were tested one by one. This required more than 15,000 file copies and scanner launches per product test. For those products that did not have an 'append to an existing file' logging option, a similar number of file copy operations were needed to preserve the report file. This testing procedure provides a more accurate indication of 'real world' detection rates. Some products are known to boost their detection rate in test situations by increasing their level of heuristic analysis once a certain number of different viruses are detected. Our test is designed to circumvent this, whilst testing products with their default settings.

The default detection settings were used, and as far as possible, all other settings were optimized to our testing procedure. Thus, memory and boot sector scanning, program self-checks, and the like, were disabled. Report logs were made, complete with missed files where possible, and the whole process automated through a series of batch files and *NetWare* login scripts. Products with separate macro scanners presented a few minor complications to the procedure. Throw in a couple of server crashes during the actual testing run and a fine time was had by all!

The test-sets were updated so that the In the Wild Boot and File sets matched the October 1997 WildList as closely as possible. The product submission date for inclusion in this review was 31 October 1997. A Web location containing a complete listing of the test-sets is included in the technical summary box at the end of the review.

Speed tests were conducted against a selection of clean files on a local hard drive. This most closely reflects 'typical' operation in the real world. The Clean test-set consists of 5500 executables, comprising approximately 540 MB. The contents have been culled from common DOS and *Windows* applications, and from publicly accessible collections of freeware and shareware utilities. As well as being a speed test, this doubles as a false positive test – there are no viruses in this collection, so none should be found.

### Alwil AVAST! v7.70.10 31 Oct 1997

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 97.7% |
| ItW File | 95.9% | Polymorphic | 100.0% |
| ItW Overall | 97.3% | Standard | 98.8% |

Slipping a couple of percentage points on the In the Wild Overall and Standard test-set ratings, *AVAST!* has made up ground on the Macro test. It is always encouraging to see a product boost its score to 100% on the Polymorphic set, which is the most technically challenging. The viruses missed from the In the Wild File test-set were mainly *Word 8* and *Excel* macro viruses, though some samples of each kind were detected, so AVAST! can deal with viruses of these types.

*Alwil's* scanner placed half-way through the field on the speed test. Although not excitingly fast, this represents quite a respectable performance, and as would be hoped, it did not claim to find any viruses in the Clean set.

| | ItW Boot | | ItW File | | ItW Overall | Macro | | Polymorphic | | Standard | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Number | % | Number | % | % | Number | % | Number | % | Number | % |
| Alwil AVAST! | 91 | 100.0% | 632 | 95.9% | 97.3% | 730 | 97.7% | 13000 | 100.0% | 806 | 98.8% |
| Command F-PROT Pro | 91 | 100.0% | 583 | 88.6% | 92.5% | 716 | 95.9% | 7138 | 50.8% | 730 | 92.2% |
| Cybec VET | 91 | 100.0% | 422 | 66.1% | 77.6% | 730 | 98.5% | 12998 | 99.0% | 804 | 98.4% |
| Data Fellows FSAV | 91 | 100.0% | 654 | 100.0% | 100.0% | 741 | 100.0% | 12917 | 97.6% | 819 | 100.0% |
| DialogueScience Dr Web | 89 | 97.8% | 648 | 99.2% | 98.8% | 741 | 100.0% | 13000 | 100.0% | 800 | 98.1% |
| Dr Solomon's AVTK | 91 | 100.0% | 654 | 100.0% | 100.0% | 741 | 100.0% | 13000 | 100.0% | 819 | 100.0% |
| Eliashim ViruSafe | 88 | 96.7% | 646 | 98.9% | 98.1% | 726 | 97.9% | 12962 | 97.9% | 810 | 99.4% |
| ESET NOD-iCE | 91 | 100.0% | 647 | 98.5% | 99.0% | 729 | 98.3% | 13000 | 100.0% | 816 | 99.7% |
| Grisoft AVG | 86 | 94.5% | 560 | 86.2% | 89.0% | 660 | 88.2% | 10548 | 81.0% | 572 | 78.4% |
| IBM AntiVirus | 91 | 100.0% | 654 | 100.0% | 100.0% | 741 | 100.0% | 12500 | 96.2% | 819 | 100.0% |
| iRiS AntiVirus | 90 | 98.9% | 645 | 98.8% | 98.8% | 699 | 94.5% | 12103 | 91.9% | 813 | 99.3% |
| KAMI AVP | 91 | 100.0% | 654 | 100.0% | 100.0% | 741 | 100.0% | 12917 | 97.6% | 819 | 100.0% |
| McAfee VirusScan | 91 | 100.0% | 654 | 100.0% | 100.0% | 741 | 100.0% | 12797 | 93.1% | 801 | 98.8% |
| Norman ThunderByte | 91 | 100.0% | 654 | 100.0% | 100.0% | 738 | 99.6% | 13000 | 100.0% | 799 | 98.5% |
| Norman Virus Control | 91 | 100.0% | 654 | 100.0% | 100.0% | 737 | 99.5% | 13000 | 100.0% | 813 | 99.4% |
| Sophos SWEEP | 91 | 100.0% | 654 | 100.0% | 100.0% | 741 | 100.0% | 13000 | 100.0% | 817 | 99.7% |
| Symantec Norton AntiVirus | 91 | 100.0% | 648 | 99.4% | 99.6% | 740 | 99.9% | 11498 | 87.5% | 773 | 97.0% |
| Trend Micro PC-cillin | 84 | 92.3% | 638 | 97.6% | 95.8% | 676 | 91.3% | 12383 | 93.6% | 790 | 97.4% |

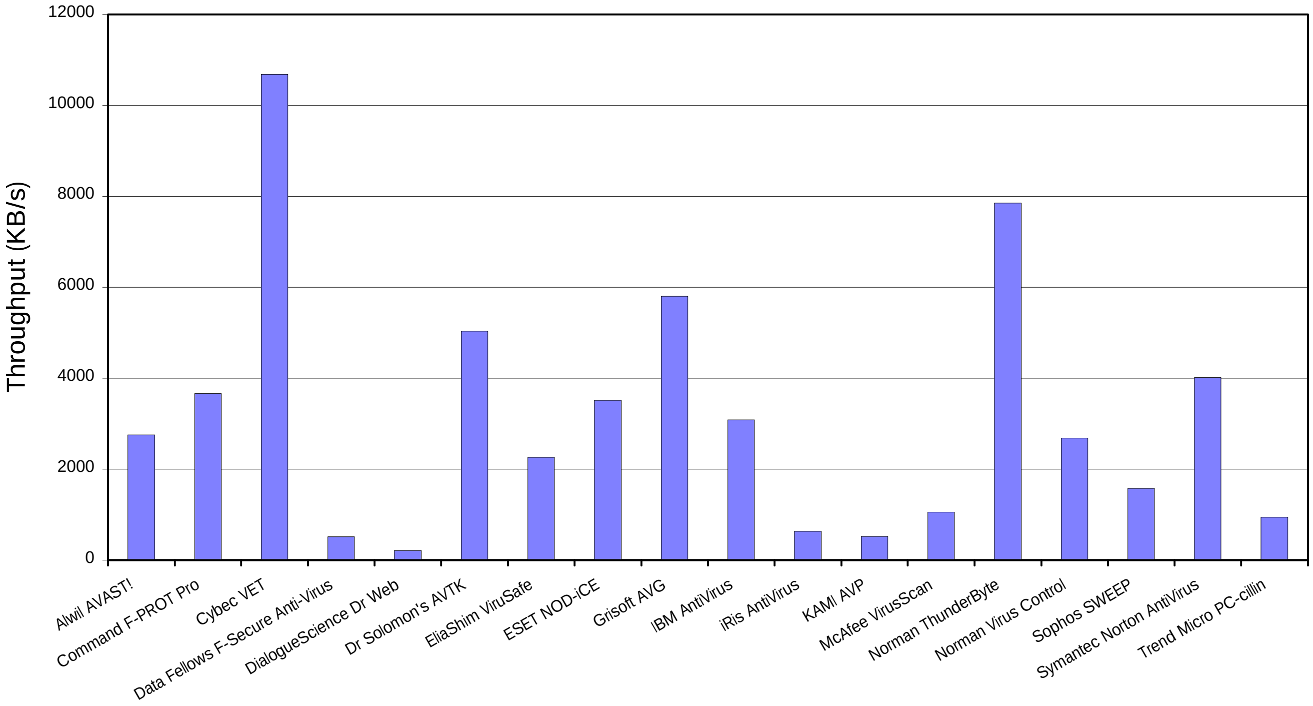
## Command F-PROT Professional v2.27a

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 95.9% |
| ItW File | 88.6% | Polymorphic | 50.8% |
| ItW Overall | 92.5% | Standard | 92.2% |

The *F-PROT* engine is currently bordering on a major upgrade, for which beta versions are in circulation. When finally released, that version should improve upon the somewhat disappointing performance seen here. *Command F-PROT Professional's* In the Wild File detection rate is depressed by the current lack of a built-in macro virus scanner, while polymorphic detection suffers from an aged emulator (an area the much-heralded v3.0 is claimed to improve significantly).

The main scanner detects many macro viruses, but does so using simple string scanning techniques. This is an unreliable approach, as the partial detection of the WM/NOP.A and WM/Pesan.B samples in the In the Wild set showed. The separate macro scanner provides much more reliable (and comprehensive) detection, although one cannot help feeling that the version supplied for review was possibly a little outdated. The v3.0 engine is also claimed to combine the macro and executable scanner. The next DOS comparative should show a marked improvement in this product.

Whilst not lightning fast, a hard disk scanning speed approaching 4000 KB/s throughput is quite nippy, placing *Command F-PROT* just in the top third of products tested. No false positives were reported.


Hard Disk Scan Rates

## Cybec VET v9.53

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 98.5% |
| ItW File | 66.1% | Polymorphic | 99.0% |
| ItW Overall | 77.6% | Standard | 98.4% |

*Cybec's VET* traditionally rates well in *VB* tests. However, the lack of any form of macro virus detection in the main DOS scanner is starting to take its toll on *VET's* detection rate against the In the Wild File set, as the proportion of macro viruses in that test-set climbs. VETMACRO , the separate macro scanner turned in a slightly improved result over its last outing against the Macro test-set, but still missed all samples of the Delta, Legend and RoboCop Excel viruses. *Cybec* has informed *VB* that it will combine its DOS macro and executable scanners in version 9.6.

Following the speed tests, *VB* staff were left wondering what the Australian developers of *VET* eat for breakfast. Typically amongst the top three speedsters, *VET* blitzed the field in this test. In outpacing its nearest rival (the traditionally speedy *Norman ThunderByte*) by more than 20%, it registered an effective data throughput rate of 10682 KB/s. Reporting no false positives, *VET* displayed a good combination of speed and accuracy.

## Data Fellows F-Secure v3.0 Build 115

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 100.0% |
| ItW File | 100.0% | Polymorphic | 97.6% |
| ItW Overall | 100.0% | Standard | 100.0% |

*Data Fellows* revamped its anti-virus software line late in 1997, combining the *F-PROT* and *AVP* scanning engines. The resulting product line goes by the name of *F-Secure Anti-Virus (FSAV)*, and this is its first appearance on any platform in a *VB* review. In the *FSAV* DOS scanner, *Data Fellows* has elected to include only the *AVP* engine. This accounts for the notable improvement over July's performance, resulting in a VB 100% award. Registering 100% against all but the Polymorphic test-set does not leave much room for further progress against the current *VB* test-sets.

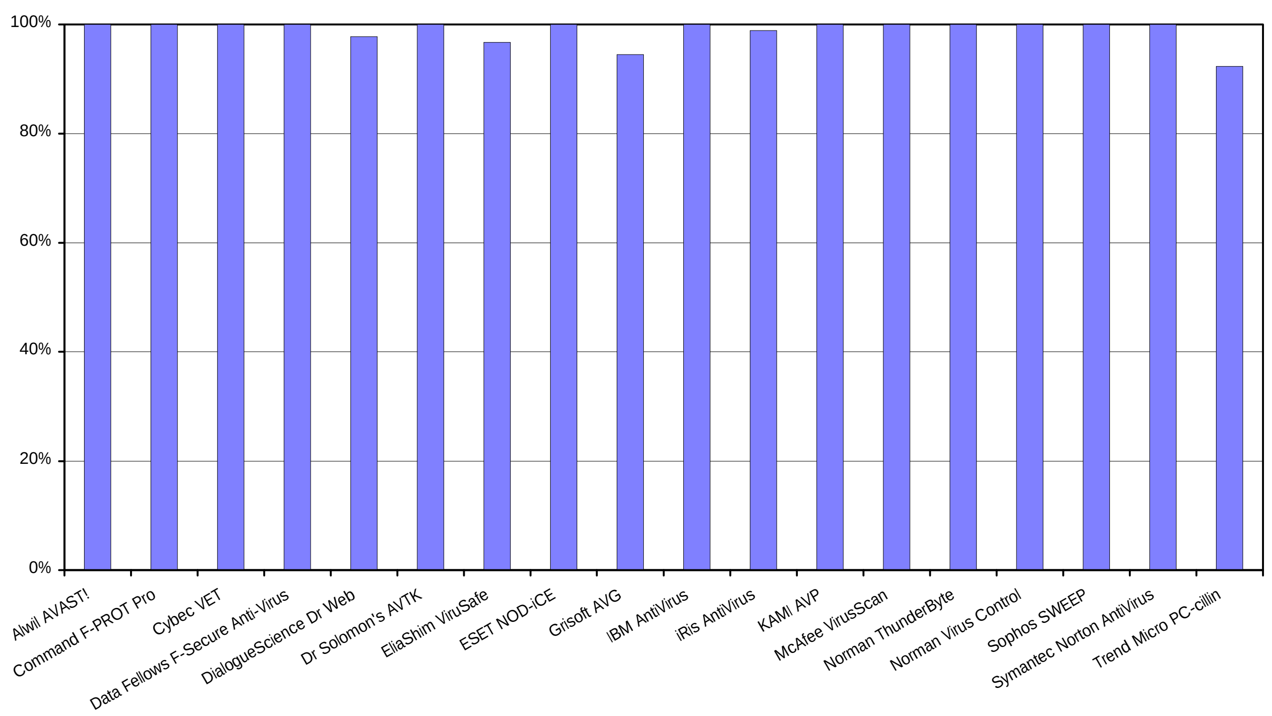
This high detection rate comes at quite a price in terms of speed, however. At less than 5% of the scan speed of *Cybec's VET*, *FSAV* was in the slowest quarter of products, though still twice as fast as the slowest.

## DialogueScience Dr Web v3.26 28 Oct 1997

| | | | |
|---|---|---|---|
| ItW Boot | 97.8% | Macro | 100.0% |
| ItW File | 99.2% | Polymorphic | 100.0% |
| ItW Overall | 98.8% | Standard | 98.1% |

*DialogueScience* specializes in detecting 'difficult' viruses, and *Dr Web* turns in another stalwart job in the trickier sets here. With perfect polymorphic and macro detection, the other holes in detection need only a little improvement. *Dr Web* depends heavily upon heuristic analysis, and while this often allows it to find new viruses other products miss, the performance overhead is very noticeable when scanning clean files. It seems that *Dr Web* runs some portion of most

In the Wild Boot Detection Rates



program files through its emulator before ‘rejecting’ them as not infected. This results in remarkably different performance from the speed demons like *VET* and *Norman ThunderByte*. They seem to have optimized reaching the conclusion ‘there is no point going further’ and thus quickly move on when scanning clean files. *Dr Web* is quite the slowest of the packages tested, and recorded nineteen false positives in its cogitation upon the clean set.

The documentation states that the default settings are not good enough to detect some highly complex polymorphics, and suggests that extra time is needed for this on top of the standard. The *Dr Web* scanner is really designed to be used in conjunction with *DialogueScience’s ADinf* integrity checker and, working in this combination, the slow but thorough scanning would not be a major problem.

## Dr Solomon’s AVTK v7.77 13 Oct 1997

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 100.0% |
| ItW File | 100.0% | Polymorphic | 100.0% |
| ItW Overall | 100.0% | Standard | 100.0% |

At times like this it can be difficult to make reviews interesting reading. 100% against all test-sets! As for detection, what more can be said? This is the first time this has happened since we introduced the macro test-set in the July DOS comparative last year, and ony the second time in recent history that a product has swept the table in a *VB* test. The *AVTK*, of course, receives a VB 100% award!

With very little room for improvement from its last outing in a DOS comparative, this product still managed the feat. Although not the absolute fastest of scanners, *Dr Solomon’s AVTK* combines very good scanning speed with excellent detection across the board.

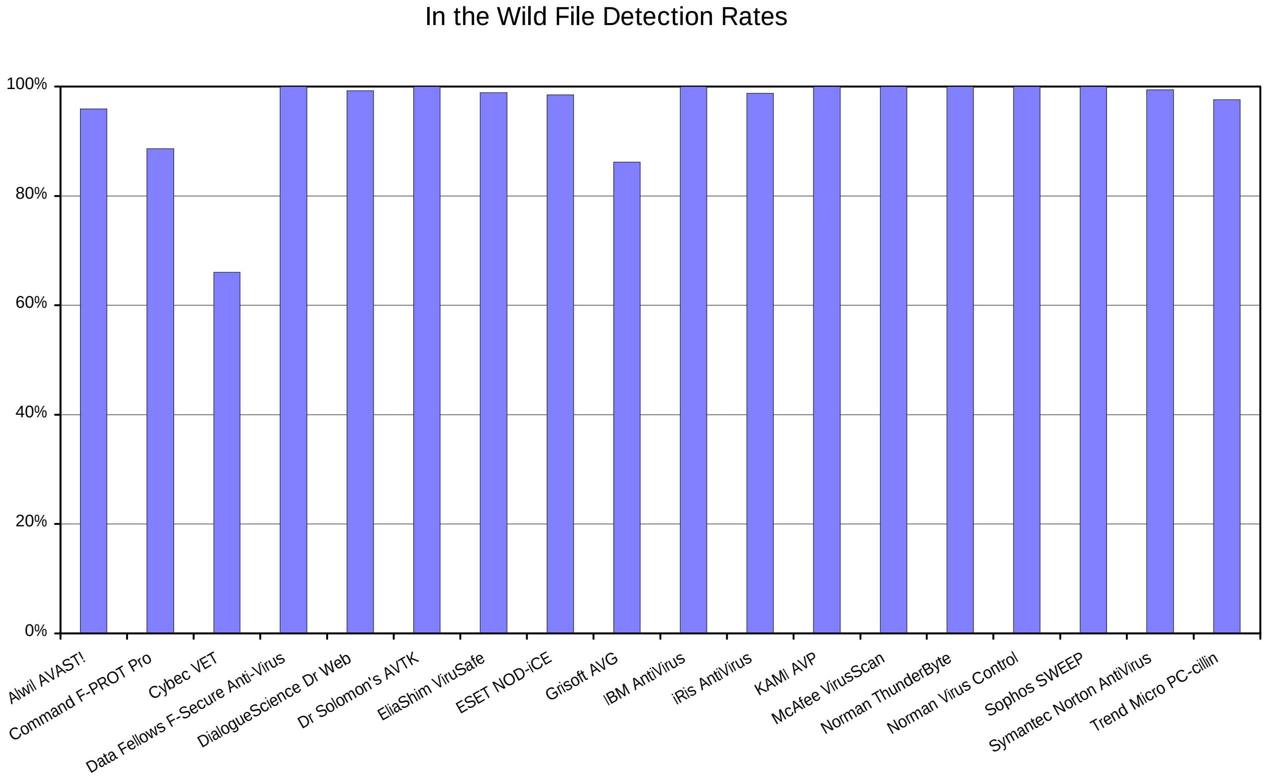
## EliaShim ViruSafe v7.53

| | | | |
|---|---|---|---|
| ItW Boot | 96.7% | Macro | 97.9% |
| ItW File | 98.9% | Polymorphic | 97.9% |
| ItW Overall | 98.1% | Standard | 99.4% |

Showing a pleasing improvement against the Macro and Polymorphic test-sets since the last DOS comparative, overall*ViruSafe* still places just out of the top rankings. A couple of relatively new macro viruses (WM/Pesan.B and WM/Schumann.C:De) blocked a perfect In the Wild File score and the three Hare variants in the In the Wild Boot test-set upset that apple-cart. In the Macro test-set it was again the comparatively new viruses (like Header.A and Mess.A) that were missed.

A more immediate cause for concern is the false positive tally of twenty-five. *ViruSafe* claimed all of them to be Cruncher.4000, so perhaps a little more work needs to be done on its definition of this virus.

While not in the top 50% of performers as far as scanning speed is concerned, *ViruSafe’s* 2263 KB/s throughput is at the respectable end of the slower half of scanners. Although noticeably slower than the real speedsters, this is probably still an acceptable scanning speed for most purposes.



## ESET NOD-iCE v7.19

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 98.3% |
| ItW File | 98.5% | Polymorphic | 100.0% |
| ItW Overall | 99.0% | Standard | 99.7% |

The first of the two new vendors to feature in this comparative review, *ESET* submitted a product that performed, perhaps surprisingly, well. We have noticed in the past how new products often take some settling in, but this has apparently already happened with *NOD-iCE*, which scored higher than some of the *Virus Bulletin* regulars. The version number presumably indicates a long development history and that the product is at least as well-established in its country of origin as any Western counterparts with similarly ‘advanced’ version numbers.

Missing some of the HLLP.5850.C, and the WM/Hiac.A and W97M/Wazzu.A samples from the In the Wild File test-set was all that stood between NOD-iCE and its first VB100% award. All are recent entrants to the top of the WildList. This must be a pleasing, if slightly frustrating, result for the product’s Czech developers. They have clearly got the fundamentals right, and we will be watching with interest to see how this product evolves over the course of future *Virus Bulletin* tests.

In terms of speed, *NOD-iCE* placed seventh fastest of the eighteen products tested, with a respectable 3514 KB/s throughput. Unfortunately, the excellent overall detection rate was offset somewhat by the detection of one ‘virus’ in the Clean test-set.

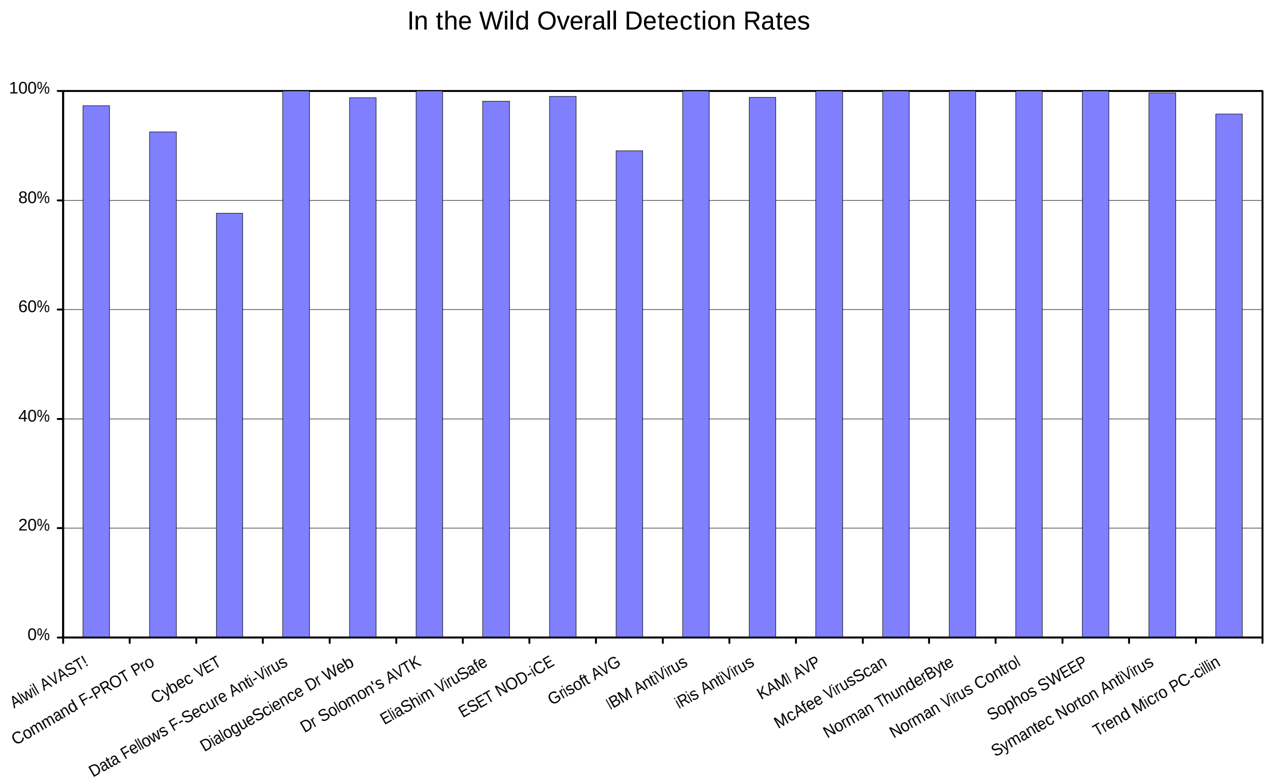
## Grisoft AVG v5.0

| | | | |
|---|---|---|---|
| ItW Boot | 94.5% | Macro | 88.2% |
| ItW File | 86.2% | Polymorphic | 81.0% |
| ItW Overall | 89.0% | Standard | 78.4% |

The other new vendor to submit a product for this review is the Slovakian anti-virus company *Grisoft. AVG* is smartly-presented, and has a notably well-translated manual. Having said that, performance with out-of-the-box settings leaves quite some room for improvement. Careful selection of scanning options can certainly result in better detection than seen in our tests, but, as usual, we tested with the default settings.

*AVG’s* relatively poor showing on the ItW File test-set was initially a little disappointing. Most of the viruses it missed entered the WildList in the two months prior to the product submission date for this test, but as usual, we used the current WildList at submission date. This, coupled with its poorer showing on the Standard test-set, suggests the developers focus on detection of ‘in the wild’ viruses. The macro viruses missed in both the ItW File and Macro test-sets were mainly new, *Word 8*, or *Excel* viruses. Detection of polymorphic viruses tended to be an all-or-nothing affair. *AVG* missed all 500 samples of each of Baran.4968, Cryptor.2582, Mad.3544 and Neuroquila.A, 452 samples of DSCE.Demo, and detected all of the rest.

As you would hope, no false positives were registered against the Clean test-set. At just over 5800 KB/s throughput, *AVG* returned the third fastest hard disk scan time. This


In the Wild Overall Detection Rates

result would likely be different should more thorough detection options be enabled by the user. *Virus Bulletin* did not formally test any of these options.

## IBM AntiVirus v3.0w

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 100.0% |
| ItW File | 100.0% | Polymorphic | 96.2% |
| ItW Overall | 100.0% | Standard | 100.0% |

*IBM AntiVirus* receives this month's third VB 100% award, their first to date. The product detected all samples of all viruses in the *Virus Bulletin* test-sets except for the 500 samples of Cryptor.2582 in the Polymorphic set.

*IBM* supplies a command-line scanner and a combined checksummer and scanner in a full-screen, menu-driven program. The command-line scanner was used for all tests in this review. The full-screen program traditionally returns very fast 'scan' speeds because it only virus-scans files whose checksums do not match those calculated on the checksummer's first run. Using the command-line scanner, *IBM AntiVirus'* scan speed was in the middle of the field. It is no surprise that no false positives were reported.

## iRiS AntiVirus v22.02 30 Oct 1997

| | | | |
|---|---|---|---|
| ItW Boot | 98.9% | Macro | 94.5% |
| ItW File | 98.8% | Polymorphic | 91.9% |
| ItW Overall | 98.8% | Standard | 99.3% |

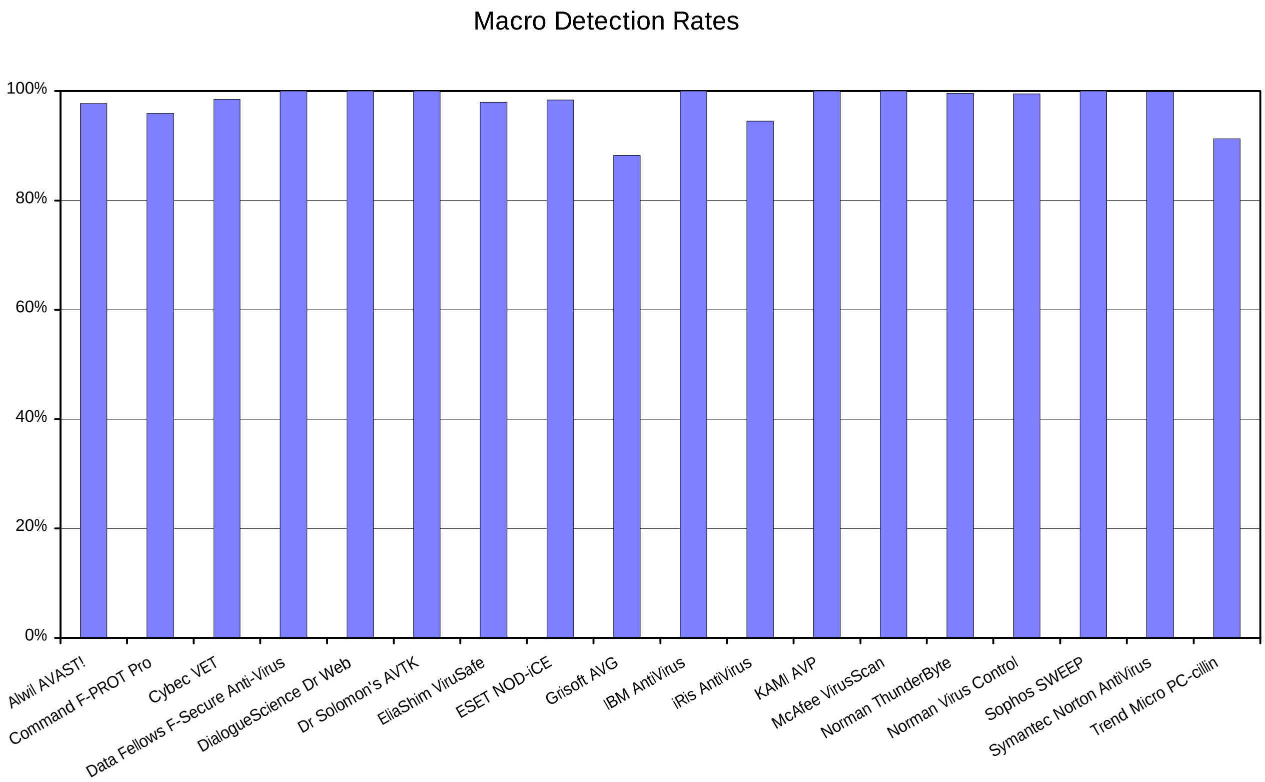
Hare.7610 from the In the Wild Boot test-set, some file replicants of its sibling, Hare.7786, and two of the macro viruses new to the WildList in October, were all iRiS AntiVirus missed from the In the Wild test-sets. This test shows a marked improvement in detection of viruses in the Macro test-set and a small improvement against the Polymorphic set, over last July's DOS comparative result. At 629 KB/s throughput, *iRiS AntiVirus* is the fourth slowest scanner on our Clean test.

The slow speed was coupled with two false positives. Normally something to be concerned about, this represents progress compared to some of the false positive results *VB* has reported from *iRiS* in the past year.

## KAMI AVP v3.0 Build 115

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 100.0% |
| ItW File | 100.0% | Polymorphic | 97.6% |
| ItW Overall | 100.0% | Standard | 100.0% |

As already mentioned, the *AVP* scanning engine is now incorporated in *Data Fellows F-Secure AntiVirus*. It should not, therefore, be surprising that *KAMI*, *AVP's* Russian developers, received the fourth VB 100% award. The results are exactly the same as for the *Data Fellows* submission, reflecting the fact that the same engine version was used in each product. The only areas of any concern in these tests were the scanning speed, a handful of Cryptor.2582 replicants and one DSCE.Demo replicant.



## McAfee VirusScan v3.1.2 13 Oct 1997

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 100.0% |
| ItW File | 100.0% | Polymorphic | 93.1% |
| ItW Overall | 100.0% | Standard | 98.8% |

Receiving this review's fifth VB 100% award, *McAfee VirusScan* has improved slightly in both its In the Wild File and Macro test-set detection rates. This continues a trend of better detection seen over the last few *Virus Bulletin* comparatives.

*VirusScan's* progress has been associated with worsening speed, and this test shows no indication of this being reversed. Recording 1059 KB/s throughput, it was the sixth slowest scanner in the pack. It reported no false positives.

## Norman ThunderByte v8.04 31 Oct 1997

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 99.6% |
| ItW File | 100.0% | Polymorphic | 100.0% |
| ItW Overall | 100.0% | Standard | 98.5% |

The first of three products to attain their second VB 100% award, *Norman ThunderByte* turned in a typically sterling performance on the In the Wild test-sets.

These results show an advance in detection of the polymorphic test-set, now fully detecting the stems it has only partially detected in previous tests. *VB's* repeated publication of test results reporting that *ThunderByte* did not fully detect SMEG_V0.3 spurred its developers in Holland to take a long, hard look at their handling of this virus. After several days work following publication of the previous DOS comparative, they reported to the *VB* editor that they had improved their SMEG detection and expected to get 100% on that stem in the next test.

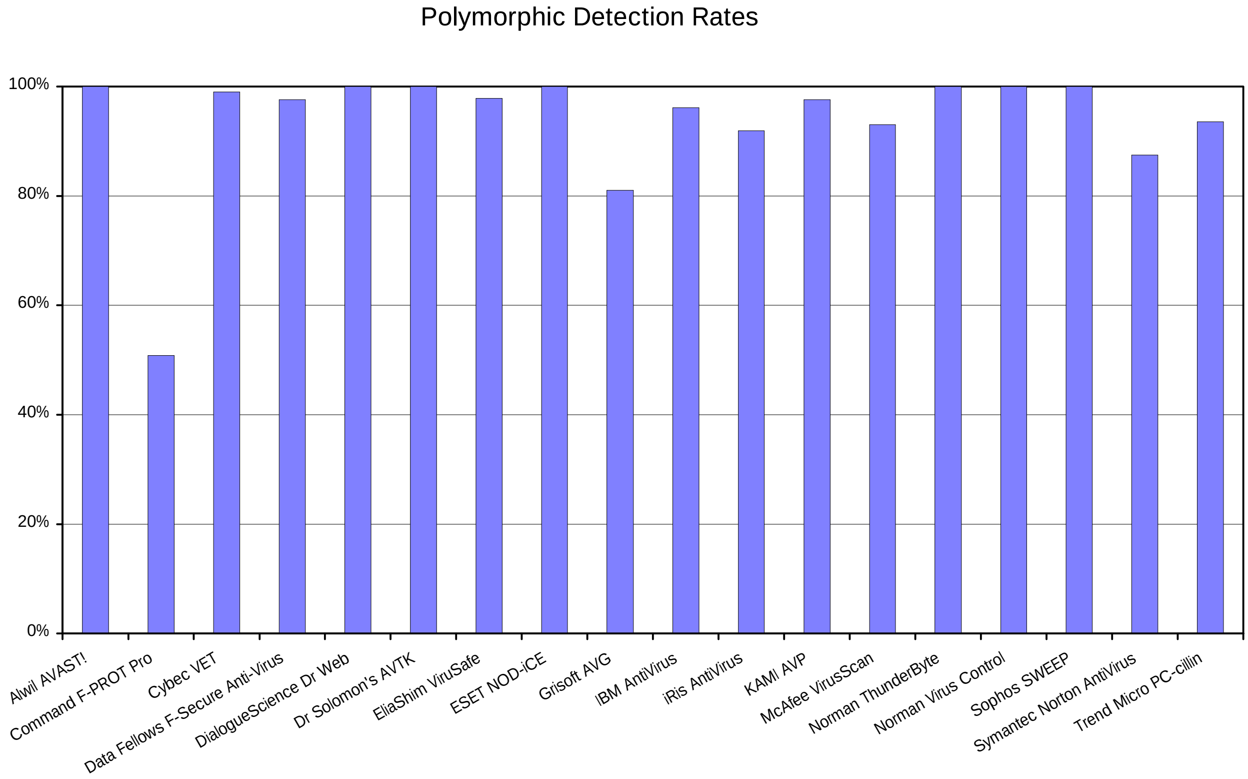
A good 30% ahead of the third fastest product, *ThunderByte* returned a scan speed of 7855 KB/s. This placed it second behind *Cybec's VET*. One false positive was reported, which marred an otherwise excellent performance.

## Norman Virus Control v4.30

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 99.5% |
| ItW File | 100.0% | Polymorphic | 100.0% |
| ItW Overall | 100.0% | Standard | 99.4% |

This VB 100% award is the second attained by the Norwegian product, *Norman Virus Control*. Its performance was every bit as commendable as that of its stablemate. Despite returning outwardly similar results, the two products use quite different scanning engines.

There was only one virus in the Macro test-set that either of the *Normans* missed, and in fact both of them missed at least some samples of it. This was the *Excel* macro virus RoboCop.A – *Norman Virus Control* missed all four samples, whereas *ThunderByte* detected one of the four. Another indication of the scanning engines being different was that *Norman Virus Control*'s scanning speed was



substantially slower. In fact, it placed right in the middle of the field, with a throughput of 2684 KB/s. Yet another pointer to differences between the products was that *Norman Virus Control* correctly failed to detect any viruses in the Clean set.

## Sophos SWEEP v3.03  3 Nov 1997

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

*Sophos* has earned itself another VB 100% award in this review, turning in near-perfect detection across the test-sets. The only virus *SWEEP* missed was both samples of Positron in the Standard set. The developers point out that *SWEEP* detects this virus in 'full sweep' mode, and they do not intend to change this.

Not surprisingly, *SWEEP* did not report any false positives in the Clean test-set. Although not the fastest scanner in this review, placing seventh slowest, *SWEEP* is faster than several of its competitors which boast similarly impressive detection rates.

## Symantec Norton AntiVirus v4.0 1 Nov 1997

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 99.9% |
| ItW File | 99.4% | Polymorphic | 87.5% |
| ItW Overall | 99.6% | Standard | 97.0% |

*Symantec* missed out on a VB 100% award by missing all the samples of HLLP.5850.D from the In the Wild File test-set. A slight improvement was seen on the Macro and Polymorphic sets, and a marked improvement was noted against the Standard test-set as compared to the results of the last DOS review in July 1997.

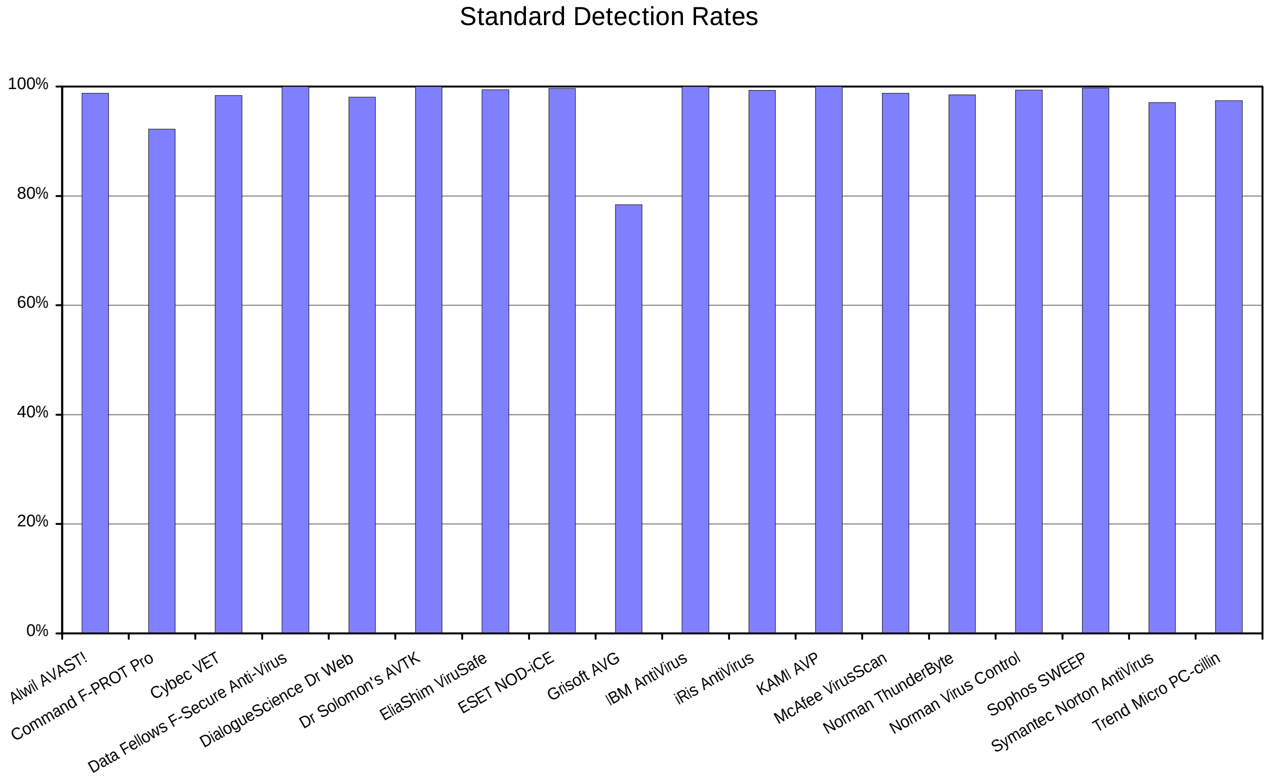
With a throughput of just over 4000 KB/s, *Norton AntiVirus* was the fourth fastest product on the scanning speed tests, notably faster than the next best performance. No false positives were reported when scanning the Clean test-set.

## Trend Micro PC-cillin v6.01  VPN 332

| | | | |
|---|---|---|---|
| ItW Boot | 92.3% | Macro | 91.3% |
| ItW File | 97.6% | Polymorphic | 93.6% |
| ItW Overall | 95.8% | Standard | 97.4% |

The first problem encountered with *PC-cillin* was that without altering the BIOS settings, it was impossible to run the program. In fact, in our test machines default configuration, this was the largest system rebooter that we have seen. The problem was resolved by enabling the 'memory hole' at the 16 MB boundary, and appeared to be associated with the DOS extender used by the product.

This apart, the results were workman-like, but not exactly thrilling stuff. Having said that, *PC-cillin* has made notable progress against *VB's* Macro, Polymorphic and Standard test-sets. However, it has slipped slightly against both In the Wild test-sets, which is interesting given that the product is listed as currently maintaining both *ICSA Certification* and



the *Secure Computing Checkmark*. This discrepancy is not peculiar to *PC-cillin*, and is normally explained by the above certification bodies using more aged WildLists as the basis of their ‘current’ tests.

No speed leader, *PC-cillin* was sixth slowest in the scan speed tests, returning a throughput of 947 KB/s. Its performance in the Clean test-set was disappointing, claiming to have found four viruses there.

## Conclusion

The relative stasis of the *Virus Bulletin* test-sets (other than the ItW Boot and File sets) over the last year is starting to show. This needs to be addressed by beefing up the non-ItW sets, which is now a priority. That said, all credit to the eight products that attained the VB 100% standard. This is as good a ‘common ground’ for required detection as the industry has. Short-listing products that consistently achieve 100% (or *very* close) detection of these viruses should be a good choice, then select based on other features.

To recap, the eight VB 100% award recipients from this review are *Data Fellows F-Secure Anti-Virus 3.0.115*, *Dr Solomon’s AVTK v7.77*, *IBM AntiVirus v3.0w*, *KAMI AVP v3.0.115*, *McAfee VirusScan v3.1.2.3010*, *Norman ThunderByte v8.04*, *Norman Virus Control v4.3* and *Sophos SWEEP v3.03*.

Special mention is due to those products scoring 100% on at least three of the four complete test-sets. These are *Data Fellows FSAV*, *IBM AntiVirus*, *KAMI AVP* and *Sophos SWEEP*. Of particular note is *Dr Solomon’s Anti-Virus Toolkit*, which scored 100% on all the *VB* test-sets – a first since adding the Macro set back in July 1997.

The days of DOS, and hence of DOS virus scanners, are probably limited now. As *Virus Bulletin’s* tests of products on other platforms have consistently shown, vendors whose DOS products score well do not necessarily score as well on other platforms. This is despite the much-repeated litany of ‘the exact same scan engine is used in all products’. Many low-level, OS technicalities complicate the issues for anti-virus software, so if you are looking for a cross-platform solution, you should choose looking at test results across all platforms of interest.

**Technical Details**

**Test Environment:** Server: *Compaq* Prolinea 590, 80 MB of RAM, 2 GB hard disk, running *NetWare 3.12.* Workstations: Three 166 MHz Pentium-MMX workstations with 64 MB of RAM, 4 GB hard disk, CD-ROM drive and a 3.5-inch floppy; One *Compaq* DeskPro XE 466, 16 MB RAM, 207 MB disk, all running MS-DOS 6.22 and *NetWare* ODI/VLM drivers. The workstations could be rebuilt from disk images and the test-sets were held in a read-only directory on the server. All timed tests were run on one workstation and it was not connected to the network for the duration of the timed tests.

**Speed and Overhead Test-sets:** Clean Hard Disk: 5500 COM and EXE files, occupying 546,932,175 bytes, copied from CD-ROM to hard disk.

**Virus Test-sets:** Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/DOS/199802/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

# PRODUCT REVIEW

## Trend Micro Server Protect for Windows NT v4.50

*Martyn Perry*

*Trend Micro's* products have often featured in *Virus Bulletin's* comparative tests, but not in a standalone review. This month we rectify that by seeing how *Server Protect for Windows NT v4.50* performs under close scrutiny.

### Presentation and Installation

To dispense with the preliminaries, a licence is required for each server on which the software is installed. *Server Protect* comes boxed with an Installation Guide, User's Guide and four diskettes. It requires a 486 or higher, with a recommended minimum of 32 MB RAM, 5 MB of disk space and *NT 3.51* or later.

The installation process has a familiar feel to it, due to the use of *Installshield*. Initially, the software scans the boot sector, and providing all is well, prompts for the licence number, which can be found on the first diskette. A destination directory is prompted for (the default is 'C:\Program Files\Trend\Sprotect'), and Select Program Group gives a choice between Create Personal Program Group and Create Common Program Group (the default). This determines whether only one person can access the *Server Protect* program group or if other users can access it. Program icons can be added now with Select Program Folder.

*Server Protect* is designed to work in a domain of servers, with one primary server that can be used to update all the others. Several options relating to these features are presented during installation. For this review I set up the test machine as an Information Server in the *Server Protect* domain TRENDTEST. The next set of options determines the scanner's initial configuration. For example, Configure Server Protect gives a choice of actions to take in the event of virus detection. There is also an option to set up the real-time scan direction (Incoming/Outgoing).

After answering all the configuration questions, program files are copied and registry entries changed. Before completing installation, it is necessary to logon to an account, either by default with Default System Account, or with a password to a specific account. At this stage, the program group shows the ISUtilty icon (for Information Server management) and the *Server Protect* icon.

The installation guide appears to have been created independently from the software, or perhaps for a different version, as there are obvious inconsistencies. Fortunately, this does not cause any problems since the installation options are fairly self-explanatory.

### Server Protect for Windows NT v4.50

*Server Protect* can provide domain management for servers. These domains are grouped under specific 'Information Servers' (IS), which sit at the top of a control hierarchy. Each IS is responsible for storing the configuration of all the domains included in its group, and for validating the password, user name and any logon restrictions.

With so much of the domain management functionality focused on Information Servers, it is good to see that *Trend Micro* makes a safety provision whereby the IS can be backed up periodically and the time interval set to hours, minutes and seconds. In addition to this, there is a separate utility (ISUtility) for managing Information Server functions which include assigning a new IS, merging existing ones, backing them up, and rebuilding.

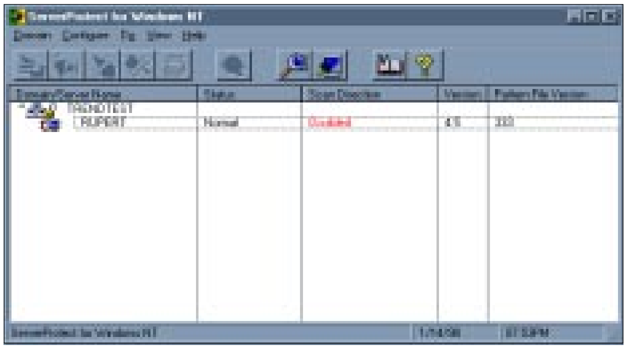
### Scanning Options

The default file extensions are BIN, COM, DLL, DOC, DOT, DRV, EXE, OVL, SYS, XLS. Additional file selections can be made or all files checked. There are separate options for boot sector scans and archived files compressed with ZIP, LHA, ARJ, and MS-COMPRESS formats.

There are several actions available for infected program files. Leave Alone performs no action on the file, Clean allows the product to attempt to remove the virus, and Rename changes the file extension to VIR, or to a user-defined one. Further options include Delete, which erases the infected file, and Move, which moves it to the directory (default 'C:\ Program Files\Trend\Sprotect\SUSPECT')

You must select Manual Scan from the Do menu in order to choose a particular directory to scan. You can then browse, choosing from Selected Drives and Directories. It is also possible to make configuration changes at this point, if required. The scan is then started.

There was a problem with the test software in that if it was required to scan only selected drives or directories, this did not seem to work as it would only check the hidden system files and the last directory on drives C and A.



| Domain/Server Name | Status | Scan Direction | Version | Pattern File Version |
|---|---|---|---|---|
| TRENDTEST | | | | |
| RUPERT | Normal | Disabled | 4.5 | 333 |

ServerProtect for Windows NT 1/14/98 07:53PM

When running, the scan display keeps incrementing totals of files scanned and infections found. Further to this, the current directory and file name under investigation are shown with an elapsed time display and progress bar. I think this is a very good set of feedback data, since it allows the supervisor to monitor, pause or curtail the scan progress if need be. Another good control feature is the option to select actions (Clean, Delete, Rename and Move) at scan time. If this is not required, then the action can be automated by selecting the appropriate action on the Manual Scan Configuration screen.

The frequency of scheduled scans can be set to Daily, Weekly or Monthly. Multiple scheduled scans can be configured and set to run concurrently, while the status of any pending scheduled scans can be viewed in the server status window. The file type and action settings available here are the same as for on-demand scanning.

Real-time scanning is available with incoming, outgoing, or incoming and outgoing scan checks. The default file extensions are the same as for Immediate scanning. In addition to using pattern file comparison for virus detection, there is an option to select behaviour monitoring. On the evidence of timing tests, this added a further 10% to the real-time scanning overhead.

### Administration

*Server Protect's* configuration utility is password-protected. Unless the correct password is entered, no configuration is enabled. The same password facility must be used each time *Server Protect* is started, even if the user is logged in with Administrator rights. This provides an additional security layer.

The configuration of each server can be defined separately, or migrated from an existing server configuration. Main menu options deal with domain management, configuration of the three scanner modes, Immediate scanning, pattern updates, and viewing the server status and log files. There is also an on-line Virus Encyclopædia.

### Reports and Activity Logs

The Manual Scan Monitor displays scan activity, showing individual files as they are scanned, along with the elapsed time and a progress bar. A log file records infections, scan summaries and pattern updates. To help filter the volume of data produced, selections can be disabled and the start and end event times are selectable. The results may be displayed on-screen, printed, or exported to a CSV file, suitable for importing into a spreadsheet, database or other report generator. This log file is quite separate from *NT's* Application Event log which can be viewed independently from within the software.

There are several methods of posting notifications of a virus incident – Message box, Printer, Pager and Internet email. Any or all can be selected and configured. The Message box option notifies selected Server(s) with a dialog box on the console. Numeric Pager support can be configured to run through a particular COM port and modem. In the case of Printer notification, text messages can be sent to designated printers, while the Internet email option sends a predefined warning message to selected users across the Internet. With this last option, there is a connectivity test facility to send the warning message as configured. The text of Message Box, Printer, and Internet email messages can be combined with special abbreviations to display virus name, user name, PC and so on.

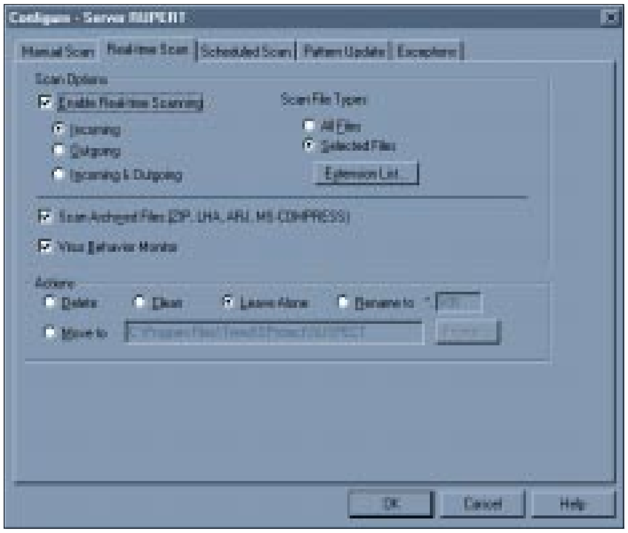
### Detection and Speed Tests

The Virus Pattern File used for testing purposes was LPT$VPN.333. Pattern files can be obtained from *Trend Micro's* BBS or FTP sites, on floppy disk or from another *Server Protect* server.

It took *Server Protect* 248 seconds to scan a floppy disk comprising 26 EXE and 17 COM files. When the test was repeated with the same files infected with Natas.4744, it took 292 seconds. The overhead was 17.7%.

It took 11 minutes and 8 seconds to scan the 5500 files of the *Virus Bulletin* Clean test-set. Unfortunately seven false positives were reported in this test. *Trend Micro* has included in their software a feature called Exception Lists, ostensibly to help overcome problems with false positives. This facility enables users to catalogue files which are not to be monitored for viruses. Normally this list is empty, but in some circumstances, as in the case of false positives, files added to this will not be monitored. There are two types of Exception List – Exception File List and Exception Pattern List. Patterns listed in the latter are not used when scanning for viruses.

The scanner was tested against the *VB* In the Wild Boot, In the Wild File, Macro, Polymorphic and Standard test-sets. Details can be found in the product summary box. The various tests were conducted using the default scanner file



Configure - Server RUPERT

Scan Options

☒ Enable Real-time Scanning

● Incoming

○ Outgoing

○ Incoming & Outgoing

Scan File Types

○ All Files

● Selected Files

☒ Scan Archived Files (ZIP, LHA, ARJ, MS-COMPRESS)

☒ Virus Behavior Monitor

Actions

○ Delete ○ Clean ● Leave Alone ○ Rename to

○ Move to

extensions, and the scan action was set to delete infected files. The residual file count was then used to determine the detection rate. Results on the In the Wild Boot tests were the most disappointing, with seven out of the ninety viruses missed –15_Years, Cruel, Hare.7750, Moloch, Neuroquila, QRoy and Satria.A.

The scanner also suffered in the Polymorphic tests, missing all 500 samples of Cryptor.2582, 116 samples of Gripe.1985 plus three other samples. Seven samples from four viruses were missed in the In the Wild File test-set (the viruses were Hare.7610, Hare.7750, Scitzo, Tentacle.II). A further 31 samples were missed in the Standard test-set. *Server Protect's* detection in the Macro test-set was much better, at 100%.

### Real-time Scanning Overhead

To determine the impact of the real-time scanner on the server's performance, the following test was performed. Two hundred COM and EXE files (totalling 20.6 MB) were copied from one folder to another using XCOPY. The folders used for the source and target were excluded from the virus scan so as to avoid the risk of a file being scanned while waiting to be copied.

The default *NT* setting of Maximum Boost for Foreground Application was used for consistency in all cases. Due to the different processes which occur within the server, the time tests were run ten times for each setting and an average taken. See the table for detailed results.

The test conditions were:

- Program not loaded. This establishes the baseline time for copying the files on the server.
- *Server Protect* service only. This shows the impact of the Domain service on its own.
- Program loaded but not scanning and Resident Protection not enabled. This tests the impact of the application in a quiescent state.
- Program loaded and Resident Protection enabled. Incoming Opening Files and Closing Files both set to 'off'. This tests the impact of having the monitor software loaded with no monitoring.
- Program loaded and Resident Protection enabled for Incoming Files only. This tests the impact of the scan on incoming files.
- Program loaded and Resident Protection enabled for Outgoing files only. This tests the impact of the scan on outgoing files.
- Program loaded and Resident Protection enabled for Incoming and Outgoing Files. This tests the impact of the scan for incoming and outgoing files.
- Program loaded and Resident Protection enabled for Incoming and Outgoing Files. Manual scan running. This tests the full impact of the scan for incoming and outgoing files as well as the normal scanning of files.
- Program unloaded. This is run after the server tests to check how well the server is returned to its former state except for the Domain service.

Activating the real-time scanner enables the behaviour monitor. The impact of the *Server Protect* service is due to the domain management software running as a service. From the results, it looks as if the on-demand scan takes over from the real-time scan, when selected.

### Summary

*Server Protect's* scanning results, apart from macro detection, need a little attention. Also, the number of false positives it detected seems worse than average. However, scanning speed is good and the configuration options are comprehensive and easy to set up. The User's Guide is concise, making it quick to locate required information . Overall, the product has a good set of facilities for managing a domain of servers in a *Windows NT* environment.

## Trend Micro Server Protect for NT

Detection Results

| Test-set[1] | Viruses Detected | Score |
|---|---|---|
| ItW File | 639/646 | 98.9% |
| ItW Boot | 83/90 | 92.2% |
| Standard | 769/799 | 96.2% |
| Macro | 741/741 | 100.0% |
| Polymorphic | 12381/13000 | 95.2% |

Overhead of On-access Scanning:

Time in seconds to copy 200 COM and EXE files (20.6 MB), averaged over ten runs.

| | Time | Overhead |
|---|---|---|
| SPNT not loaded | 19.8 | – |
| SPNT Domain service only | 20.3 | 2.5% |
| — + inactive resident scanner | 20.8 | 5.1% |
| — + resident scan, incoming | 21.3 | 7.6% |
| — + resident scan, outgoing | 21.6 | 9.1% |
| — + resident scan, both | 21.8 | 10.1% |
| — + — + on-demand scan | 20.9 | 5.6% |
| SPNT unloaded | 20.6 | 4.0% |

**Technical Details**

**Product:** *Trend Micro Server Protect for Windows NT v4.50.*

**Developer/Vendor:** *Trend Micro Inc,* 10101 De Anza Blvd,
4th Floor, Cupertino, California 95014, USA.
Tel 1 800 228 5651, fax +1 408 257 2003,
email: trend@trendmicro.com, WWW http//www.antivirus.com/.

**Price:** List price for 50 users, $1150.

**Hardware Used:** *Compaq* Prolinea 590 with 80 MB RAM, 2 GB hard disk, *NT* server 4.0 with service pack 3.

[1]**Test-sets:** Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/DOS/199802/test_sets.html.

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

### SUBSCRIPTION RATES

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

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

**Editorial enquiries, subscription enquiries, orders and payments:**

*Virus Bulletin Ltd*, 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:**

*Virus Bulletin*, 18 Commerce Way, Woburn, MA 01801, USA

Tel (781) 9377768, Fax (781) 9320251

# END NOTES AND NEWS

**A practical *NetWare* security course** will be held at the *Sophos* training suite in Abingdon in the UK on 19 March 1998. **An introductory computer virus workshop** takes place at the same site on 17 March, followed by an advanced session on 18 March. Contact Karen Richardson; Tel +44 1235 544015, fax +44 1235 559935, or visit the company's Web site; http://www.sophos.com/.

***Symantec's* long-running claim of copyright violation against *Network Associates*** ended late last year. A United States District Court denied the request for an injunction against *McAfee PC Medic*, when *Symantec's* expert testified that the code in question was 'substantially and fundamentally different' from his company's own. *Network Associates* has followed the move by dropping its defamation suit against *Symantec.*

***Dr Solomon's Anti-Virus for Microsoft Exchange,*** released at the end of December 1997, retails from £395 excluding VAT. It automatically detects and disinfects viruses in *Microsoft Exchange* mail folders with a notification service and a quaratine option. In addition to the server software *Dr Solomon's Mailbox Scanner*, 32-bit scanners for MS-Mail, MS-Exchange and MS-Outlook, provide real-time and scheduled email scanning. Contact Rosemary Bladon; Tel +44 1296 318700, or email pr@uk.drsolomon.com.

***WebSec '98*: The Conference on Web, Internet & Intranet Security** will be held at London's Cumberland Hotel from 10–12 March 1998. In addition to the accompanying exhibition, there are optional workshops on 9 and 13 March. The conference focuses specifically on Web and Internet management and security, infrastructure and internetworking. Contact *MIS* for details; Tel +44 171 779 8944, email drosen@misti.com or visit their Web site at http://www.misti.com/.

***Norman Data Defense Systems* has released a server-based product to detect and clean viruses in *Lotus Domino* databases.** *Norman Virus Control for GroupWare* has real-time and on-demand scanning functionality and also cleans macro viruses 'on the fly'. This means that *Word* and *Excel* documents coming from a *Domino* server are cleaned automatically before being opened. The product has powerful alarm and logging options, and a quarantine option. The developers claim that the overhead is negligible. For more information contact *Norman's* President Gunnel B Wullstein; Tel +47 67589930.

***Peapod Internet* is to distribute *Trend Micro's InterScan VirusWall* for *Lotus Messaging Switch* (*LMS*) *3.0*.** Email attachments are automatically scanned 'on the fly' at the *LMS* server. Messages carrying viruses are rejected and the administrator and sender are alerted. The virus scan feature is built in as an option on each *LMS* and is available by emailing trend@peapod.co.uk with *LMS* in the header. Pricing starts at £895 for 50 users.

***Network Associates* has introduced *NewsSniffer*,** the first service to scan *all* Usenet newsgroup messages for viruses. The service checks message attachments, scanning continuously for new viruses, alerting and advising users on detection. *Network Associates* claims that *NewsSniffer* scans all current Usenet newsgroups free of charge. Contact Caroline Kuipers for more information; Tel +44 1344 304730, fax +44 1344 306902, or email caroline_kuipers@cc.mcafee.com.

***Reflex Magnetics Ltd* will hold a two-day *Live Virus Experience*** from 10–11 February 1998. The workshop, to be run by Dr David Aubrey-Jones, takes place at the company's offices in London. It provides experience in detecting and controlling viruses on PCs, with a particular focus on macro viruses. For more details contact Rae Sutton; Tel +44 171 3726666, fax +44 171 3722507 or email rae.sutton@reflex-magnetics.co.uk.

***Network Associates* has angered Israeli anti-virus developer *iRiS Software*.** As reported on the News page of the December 1997 issue, *iRiS* has released a *Windows CE* virus scanner. Thus, a recent *Network Associates* (formerly *McAfee Associates*) press release claiming that the California-based company would be the first to offer virus protection for *Windows CE* users, prompted a swift rejoinder from Tel Aviv. *Network Associates* was 'just a little too late' to claim this initiative chuckled Alan Komet, *iRis'* marketing manager. *Virus Bulletin* also notes with interest that *Network Associates* has entered the vapourware market – the January press release in question clearly states that it 'would develop' a *Windows CE* version of *VirusScan*, but this does not prevent *Network Associates* claiming to be 'the first company to offer' such a product.

***Virus Bulletin* announces the call for papers** to be considered for inclusion in the VB'98 Conference programme. For contact details, please refer to the announcement on p.3.