ISSN 0956-9979

MAY 1997

# VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

Technical Editor: **Jakub Kaminski**

Assistant Editor: **Megan Skinner**

Consulting Editors:

**Richard Ford,** IBM, USA
**Edward Wilding,** Network Security, UK

## IN THIS ISSUE:

• **Window cleaning again!** This month sees the second *VB* comparative review of anti-virus software for *Windows 95*. What has changed in the past year? What is new on the market? Turn to p.11 for the lowdown.

• **Fronting the issue.** This month's editorial has been written by our Technical Editor, Jakub Kaminski – a man of strong opinions! Read his views on p.2.

• **Insightful revelations.** Since leaving *Virus Bulletin* just two years ago, Richard Ford has followed a complex career. Now settled at *IBM*, he discusses the route which led him there – see p.6.

## CONTENTS

**GUEST EDITORIAL**

**NEWS**

**INSIGHT**

**VIRUS ANALYSIS**

**COMPARATIVE REVIEW**

**PRODUCT REVIEWS**

VIRUS BULLETIN ©**1997 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England.**
**Tel +44 1235 555139. /97/$0.00+2.50** No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

# GUEST EDITORIAL

## Playing the Game

What do competitors do? It seems obvious – they compete; they try to be better than other players. In the trade world it means delivering better products, providing better service, being more attractive to current and potential customers. Unfortunately, being good (or even very good) is not good enough if only few know about it. In these days when the anti-virus industry is flooded with products and promises, marketing professionals must work hard to make their claims stand out from the rest of the info-mercial gargle. The art of marketing and advertising has reached an astonishing level. Saying 'We're the best' is a must, but it doesn't convince anyone any more. One can achieve much better results with the old dirty trick; saying how bad others are. Moreover, finding faults in another product is quite easy, and announcing them loudly guarantees attention (even if only from those challenged).

*“it looks silly to condemn a method that results in a better detection rate”*

During early April we saw a war of press releases between two companies holding significant shares of the anti-virus market – *McAfee* and *Dr Solomon's Software* (*DSSL*). Accusations were stated, the response was quick, the response to the response followed, and the response to the response to the response, as sadly expected. The reasons triggering the first statements look obvious (see above) but what were the issues of the discussion (at least the initial part)? The facts can be summarized thus:

- the scanner provided as a part of *Dr Solomon's AntiVirus Toolkit* contains a curious feature; when running in default mode and after detecting eleven uniquely-infected files, it switches automatically into heuristic detection mode
- the switch prohibiting such behaviour is undocumented
- scanning a collection of viruses in one go may produce different results from scanning the same viruses one at a time (the first method may detect more viruses if a collection contains any new, previously unknown ones)

At this point most users would probably ask, 'So is this good or bad?'. To begin, *McAfee's* reaction to the above points: first, this method is a 'cheat' mode. Second, this finding '…casts doubt over the accuracy of *Dr Solomon's* detection rates and scanning speeds'. Third, '*McAfee* is not aware of any real-world end-user cases where this number of unique infections have been found on one system, so this is not an "end-user" feature. It means that the cheat mode has been specifically designed for the review purposes to show "inflated virus detection results".' Finally, some viruses detected in a collection may be undetected (in the same default mode) if placed separately on an end-user machine.

*DSSL's* initial response was: 'Advanced Heuristic Analysis is automatically enabled when Dr Solomon's detects that it is running on a highly infested computer – which means Dr Solomon's provides a higher level of detection than competitors.' Second, 'The technology is available to every user and can be manually enabled at any time'. A few other technical arguments were brought in (by both sides), ethics called into question and discussion soon deteriorated into involving third-party companies (anti-virus research and product test organizations, some of which were called by both sides) and ended up literally in an argument over who's got bigger … growth!

Members of the anti-virus community tend to argue about a number of viruses triggering the automatic switch into heuristics and the fact that the feature is undocumented. Some who've known about this feature for some time do not regard it as a big issue. It seems obvious that this specific design has more use in test reviews than in the real-user world but, equally, it looks silly to condemn a method that results in a better detection rate. As usual, one's point of view depends strongly on immediate geography. As for users, they are almost exactly where they were a few weeks ago, maybe richer in a few new technical details but probably more confused as to the significance of these details.

The main conclusion appears clear: whatever *McAfee's* reasons behind the initial attack, the final result was probably miscalculated (gently speaking). In the light of well-matched aggression and the balance of both sides' arguments, in the days where any publicity is good publicity it looks as if *McAfee* helped *Dr Solomon* attract more attention on American soil.

*Jakub Kaminski*

# NEWS

## What's Wazzu New at CeBIT 97?

A report in the German *PC Magazin DOS* describes the latest widely-distributed virus: the CD-ROM 'What's new at CeBIT 97' contained an inactive sample of Wazzu. A harmless matter, according to the article, but nevertheless embarrassing for the producers 'Hardlight Multimedia', the sponsor 'Macromedia', and the journal 'CeBIT News', which gave the disk free to visitors.

According to a *CeBIT* spokeswoman, the CD concerned contained press releases, and was distributed to at least 30,000 people as a supplement to the *CeBIT* catalogue. The first to notice the infection was Australian anti-virus specialist *Leprechaun Software*.

Eight different *Word* documents were infected; that the infection was Wazzu was confirmed at the *McAfee* stand. Throughout the exhibition, warnings about the infected CD were posted on Infostands ▮

## AOL-Not-Quite-So-Free

*Virus Bulletin* has been receiving reports about yet another virus hoax, this one going under the name 'AOL4FREE'. Reports began circulating in the early part of March, and take the normal form of such Internet virus hoaxes.

Readers should, however, note that another file, AOL4FREE.COM, contains a Trojan horse which can destroy data on the user's C: drive ▮

## Adding up the Profits

Two anti-virus software developers, *Dr Solomon's Software Ltd* and *McAfee Associates*, have once again announced record earnings, this time for the first quarter of 1997.

*Dr Solomon's Software Ltd*, for its third quarter ending 28 February 1997, has recorded an operating profit of £2.7 million, up from £1.9 million in the previous quarter and from £1.3 million in the corresponding 1996 quarter. Operating profit for the first three quarters of this financial year was £6.1 million, compared to £2.0 million in the same period the previous year, with bookings up 62%.

*McAfee*, for its first quarter ending 31 March 1997, shows revenue in excess of US$73 million, 117% above that recorded a year ago. *McAfee's* latest move in the anti-virus market is the acquisition of Japanese anti-virus developer *Jade Software*, with which the company plans to target the Far Eastern market more forcefully.

Information on each company can be found on their Web sites: *Dr Solomon's*: http://www.drsolomon.com/; *McAfee*: http://www.mcafee.com/. ▮

### Prevalence Table – March 1997

| Virus | Type | Incidents | Reports |
|---|---|---|---|
| Concept | Macro | 69 | 17.3% |
| NPad | Macro | 37 | 9.3% |
| Form | Boot | 23 | 5.8% |
| ParityBoot.B | Boot | 22 | 5.5% |
| AntiCMOS | Boot | 20 | 5.0% |
| Wazzu | Macro | 18 | 4.5% |
| AntiEXE | Boot | 16 | 4.0% |
| NYB | Boot | 15 | 3.8% |
| MDMA | Macro | 14 | 3.5% |
| Ripper | Boot | 11 | 2.8% |
| Empire.Monkey.B | Boot | 10 | 2.5% |
| Bandung | Macro | 7 | 1.8% |
| Quandary | Boot | 7 | 1.8% |
| Stoned.Angelina | Boot | 7 | 1.8% |
| Junkie | Multi | 6 | 1.5% |
| Laroux | Macro | 5 | 1.3% |
| Sampo | Boot | 5 | 1.3% |
| Showoff | Macro | 5 | 1.3% |
| WelcomB | Boot | 5 | 1.3% |
| Colors | Macro | 4 | 1.0% |
| Intruder | File | 4 | 1.0% |
| Telefonica | Multi | 4 | 1.0% |
| Cap | Macro | 3 | 0.8% |
| DelCMOS.B | Boot | 3 | 0.8% |
| Hassle | Macro | 3 | 0.8% |
| Johnny | Macro | 3 | 0.8% |
| Stoned.Spirit | Boot | 3 | 0.8% |
| Temple | Macro | 3 | 0.8% |
| Other[1] | | 68 | 17.0% |
| **Total** | | **400** | **100%** |

[1] The Prevalence Table includes two reports of each of the following viruses: AntiCMOS.B, Die_Hard, Doggie, Helper, Jumper.A, Jumper.B, Peter, Rapi, Tentacle_II, Tubo, and V-Sign.

It also includes one report of each of the following viruses: Anthrax, Boot.437, Burglar, Bye, CF.140, Cheap.828, CMP.4096, Cruel, Edwin, Eel.360, EXEBug, Hassle, Havoc.3072, Hippie, Imposter, Int40, IntCE, Keypress.1216, Kompu, Konstantin, Leandro, Maltese Amoeba, Manzon, Natas.4744, NF, NiceDay, Nightfall, NoPrint, Nuclear, Nuke.1680, Rhubarb, Sack, ShareFun, SILLYBOP, Sofa, Spanska.1120.b, Stat, Stealth_Boot.C, Stoned.NoInt, Stoned.Manitoba, Tentacle, Tequila, Trojector, Trackswap, TPVO.3783, and Unashamed.

# 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 April 1997. Each entry consists of the virus name, its aliases (if any) and the virus type. This is followed by a short description (if available) and a 24-byte hexadecimal search pattern to detect the presence of the virus with a disk utility or a dedicated scanner which contains a user-updatable pattern library.

**Type Codes**

| | | | |
|---|---|---|---|
| **C** | Infects COM files | **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 |

**Andromeda.1337**

**CR:** An appending, 1337-byte virus containing the text ‘ANDROMEDA/plus BUDAPEST 1991’. The virus’ payload includes intercepting reads of sector 1, cylinder 0, head 0; when such access is detected, Andromeda returns a chunk of code with the familiar text: ‘Your PC is now Stoned!’.

```
Andromeda.1337      BEFE CDB4 30CD 2181 FF3D 1B75 17BE 1B04 5B81 EB00 0103 F3BF
```

**Apadana.1500**

**CR:** A stealth, prepending, 1500-byte virus. On 30th of the month, the text ‘My name is APADANA I am a virus version 1.3’ is displayed. As its stealth routine triggers on the DOS Find_Next call, the reported size of the first file in a directory listing is always the true one. Infected files’ time-stamps are set to 62 seconds.

```
Apadana.1500        B821 35CD 21B4 ECCD 2180 FCCE 7503 E9AC 0089 1E98 0489 1E61
```

**Atomic.422**

**ER:** A 422-byte companion virus containing the text: ‘❊ Atomic v1.00 ❊ by MnemoniX’.

```
Atomic.422          BA00 01B9 A601 B440 E82A FFB4 3EE8 25FF 071F 5F5E 5A59 5B58
```

**BW.778**

**CER:** A stealth, appending, 778-byte virus, containing the texts: ‘[BW]’ and ‘Mess with White Shark and you’ll be eaten alive!’ All infected programs have their time-stamp set to 62 seconds.

```
BW.778              3402 E621 B806 A2CD 2181 FBE2 4174 348C C048 8ED8 832E 0300
```

**BW.786**

**CER:** A stealth, appending, 786-byte virus, containing the texts ‘[BW]’ and ‘By White Shark! Mess with White Shark and you’ll be eaten alive!’. It infects on opening. Infected files’ time-stamps are set to 2 seconds.

```
BW.786              3402 E621 B8F6 FECD 2181 FBCE C974 3A8C C048 8ED8 832E 0300
```

**DarkManko.764**

**CN:** An encrypted, appending, 764-byte, direct infector. It contains the text: ‘*.com’ and ‘JapanReseachInstituteOfSelfReproducingProgram[JRIOSRP-6]DarkManko3/5/95’.

```
DarkManko.764       8905 47E2 F6B9 4D01 8BFE 83EF 058B 0535 ???? 8905 4747 E2F5
```

**DarkRay.466**

**CN:** An appending, 466-byte, direct infector containing the texts ‘This file contains a virus!!! Please COLD-boot from a write protected system disk and use you anti virus software!!! Dit virus is ter RESEARCH en STUDIE geschreven!! Misbruik hiervan is strafbaar onder de Nederlandse wet!! (C) 1994 - [DóRkRóY] retired virus writer...’ and ‘*.COM’.

```
DarkRay.466         2E89 86D6 02B4 40B9 D201 8D96 0401 CD21 B800 4233 C933 D2CD
```

**Eel.360**

**ER:** An appending, 360-byte virus, reinfecting already-infected files. The ‘Are you there?’ call (Int 21h, AH=FEh) returns AH=0h if the virus is active in memory.

```
Eel.360             B4FE CD21 0AE4 745B 1E8C D848 8ED8 8A16 0000 C606 0000 4D8B
```

**EVC.161**

**CER:** An overwriting, 161-byte virus containing the text: ‘EVC 1.04’ and ‘Virus By White Shark’. The latter is displayed on the seventh day of every month.

```
EVC.161             B440 B9A1 008E 1E4B 01BA 0001 2EFF 1E47 01B4 3E2E FF1E 4701
```

**Fuga.969**

**CER:** An overwriting, 969-byte virus marking all infected files with byte 88h at offset 0003h (COM) and 0013h (EXE). It contains a payload which triggers in March and displays the text (in blinking white text on a red background): ‘<——— ERROR CRITICO: Fuga de prsión en el monitor’.

```
Fuga.969            B888 88CD 213D 05CA 7517 B90E 00FC 0E1F BEBB 038B FE03 F5F3
```

**Grosser.607**

**CN:** A prepending, 607-byte direct infector containing the text: ‘*.com’, ‘0000 virus’, ‘Virus 0000.0000 Created by GROSSER (C) 1996 AUGUST’, ASSEMBLER’, PASCAL’, ‘BASIC’.

```
Grosser.607         72D3 B440 BA00 01B9 5F02 CD21 72C7 BF80 00BE 68F2 90B9 0001
```

**Henon.721**

**CN:** An appending, 721-byte direct infector containing the text ‘DeViANT MiND’ at the end of infected files. The virus infects one file at a time, and also contains encrypted text, displayed on Mondays: ‘*******Ever wished there was something more to your life? A bit of serendipity, spontenaety, randomness.. Maybe even a tiny bit of demented chaos? Well buddy, if you want demented chaos, you’ve got it. Welcome to Henon2 - The Edge of Chaos DeViANT MiND *******’ and ‘Punch a key to continue...’.

```
Henon.721           B440 8D96 1701 B9D1 02CD 21B8 0157 8B8E A202 8B96 A402 CD21
```

**Joan.480**

**ER:** An appending, 480-byte virus infecting drivers with extension ‘sys’. It contains the text ‘ Joan v6.23 by KiKo NoMo Happy Birthday to you, Joan KiKo’ – this should be displayed on 15 April; a bug means it is not.

```
Joan.480            0242 33C9 99E8 2900 B440 B9E0 01E8 2100 45B4 3EE8 1B00 B44F
```

**Luri.1217**

**ER:** An appending, 1217-byte virus containing the text '(C) May 4th 1993By Luri DarmawanSemarang - 50112— Indonesia. —'. This message is stored in the boot sector, and displayed when a system is booted from a disk corrupted by the  virus.

```
Luri.1217           B440 8B1E 8801 B9C0 04BA 0001 CD21 721D B800 428B 1E88 0133
```

**Minimad.279**

**CN:** An appending 279-byte direct infector containing the text 'The MiniMad version 1.0 beta*.com'. A slightly-corrupted, but still replicating, minor variant is also known.

```
MiniMad.279.A       BA53 0A03 D5B9 1701 903E 8B9E 660B CD21 582E 8986 640B 33C9
MiniMad.279.B       BA53 0A03 D5B9 1701 903E 8B9E 660B CD21 CC2E 8986 640B 33C9
```

**Nado.807**

**CR:** A stealth, encrypted, appending, 807-byte virus containing the text: 'Nicolai C. version 1.00E'. All infected files have their time-stamps set to 2 seconds.

```
Nado.807            3E8B 96FF 028D B609 00B9 6501 3114 4646 E2FA C3E8 0000 5D81
```

**Oolong.1386**

**CER:** An appending, 1386-byte virus containing the text 'Oolong V2.0 virus by [E.K]'. Infected COM files start with byte E9h (near jump), and EXE files have the word 454Bh ('KE') at offset 0012h.

```
Oolong.1386         B440 B96A 05BA 0001 9C2E FF1E 0506 7220 B800 4233 C999 9C2E
```

**Qpa.666**

**CN:** An overwriting, 666-byte virus which stores the host file's original initial 666 bytes in a hidden file with the same name but the extension: 'win'. The virus contains the texts 'Qpa-XXI virus V1.0 from', '*.C[93h]M', 'This program requires Microsoft Windows.' and 'EOV'.

```
Qpa.666             BAB3 03B9 9A02 90B4 40CD 213B C173 03E9 38FF B43E CD21 7303
```

**Reu.1367**

**CER:** An appending, 1367-byte virus containing the text: 'Written in the city of Istanbul (c)1994 by REUIUKRGT'. When active in memory, the virus truncates the length of certain EXE files executed to zero bytes (e.g. X.EXE, CIV.EXE, WOLF3d.EXE).

```
Reu.1367            B824 4BCD 213D 3434 7457 E8A9 0274 522E A12F 0406 488E C026
```

**Sepultura.242**

**CR:** An appending, 242-byte virus containing the texts '[242]' and 'Sepultura'. Infected files have their date and time-stamps set to 00-02-42, 2:42:00.

```
Sepultura.242       B909 006A 00E2 FC61 B842 02CD 21E8 0000 5E83 EE10 BF42 0207
```

**Spanska.1000**

**CN:** An encrypted, appending, 1000-byte, direct infector. Its payload triggers between 22 minutes and 22 minutes 30 seconds past every hour and displays the message: 'Remember those who died for Madrid No Pasaran! Virus v2 by Spanska 1997'. Infected files have the word 636Ch ('lc') at offset 0003h.

```
Spanska.1000        C38A 96F6 04B9 B303 8DB6 3E01 8BFE 8A04 4632 C2E8 D5FF E2F6
```

**Spanska.1120.A**

**CN:** An encrypted, appending, 1120-byte, direct infector infecting up to seven files at a time. Its payload triggers between 22 minutes and 22 minutes 30 seconds past every hour and displays the message 'Remember those who died for Madrid No Pasaran! Virus (c) El Gato 1996'. The text is accompanied by two torches burning in the bottom corners of the screen. Infected files have the word 626Ch ('lb') at offset 0003h.

```
Spanska.1120.A      ACEB 01?? 32C2 80FA 0074 0732 8643 01EB 01?? AAEB 01?? E2E4
```

**Spanska.1120.B**

**CN:** An encrypted, appending, 1120-byte, direct infector infecting up to six files at a time. It contains a payload which triggers between 52 minutes and 52 minutes 20 seconds past every hour and displays the message 'To Carl Sagan poet and scientist, this little Cosmos. (Spanska 97)' on the background of passing stars. Infected files have the word 6161h ('aa') at offset 0003h.

```
Spanska.1120.B      0547 C38A 9621 01B9 3404 8DB6 3B01 8BFE AC32 C2E8 E9FF E2F8
```

**Squad.1299**

**CER:** An encrypted, appending, 1299-byte virus containing the texts 'This virus is a publicity stunt of the DOG SQUAD (CSE 93 Batch of RECJ) and has been issued in public interest by the Registar of the Squad. Long Live N.P.' and '.COM','.EXE', '.C', '.CPP', '.PAS', '.TXT', '.PRG'.

```
Squad.1299          50E8 0000 0E1F 5B81 EB0E 0188 8719 018D BF26 01B9 F204 8035
```

**Tangle.378**

**CN:** An encrypted, appending, 378-byte direct infector which infects files singly. It contains the text '*.com'. All infected files have byte 32h ('2') at offset 0003h.

```
Tangle.378          8B3E 0101 EB01 EA81 C734 018B F7B9 4901 B4?? EB01 EAAC 2AC4
```

**Uniba.334**

**CN:** An appending, 334-byte, fast, direct infector containing the texts '[Pandora II ALPHA]', 'Blood Mary', 'Soochow Uni.B.A.', '*.COM' and '????????COM'. Infected files have the word 5032h (2P) at offset 0003h.

```
Uniba.334           6C75 ED80 7D04 7775 E787 D7B8 2125 CD21 0E1F 8DB6 1202 BF00
```

**Virdem.836**

**CN:** A prepending, 836-byte direct infector, containing the encrypted texts '*.com', 'COMM' and 'There are 3 rules to obey Keep them out of sunlight Dont get them wet Never feed them after midnight You disobeyed one rule'.

```
Virdem.836          B440 B944 038D 1600 01CD 21B8 0242 BA00 00B9 0000 CD21 B440
```

**VT.720**

**CER:** An appending, 720-byte virus. Its 'Are you there?' call (AX=4B6Ch ['lK'], Int 21h) returns a value of AX=5456h ('VT').

```
VT.720              B800 4259 5ACD 21B4 40B9 D002 33D2 CD21 B801 57BC E005 595A
```

**Warp.174**

**CER:** An overwriting, 174-byte virus containing the texts 'VoFca' and 'EXEC failure'. The latter is displayed when a new file is executed.

```
Warp.174            3D41 5775 04B8 5052 CF80 FC4B 7527 5053 5152 1EB8 0143 33C9
```

**Xingo.1308**

**CER:** An appending, 1308-byte virus.

```
Xingo.1308          3DFF FF75 05B8 8880 EB18 80FC 4B75 03E8 1300 80FC 4074 0580
```

## INSIGHT

# Fording the Atlantic

Wellington is a name which people might more readily associate with military heroes, or a fine meal, than with anti-virus researchers. There is, however, a link – Wellington is an English market town, where Richard Ford grew up.

Ford hails from a traditionally English background: his father, a schoolteacher, stimulated a boyish interest in how things work. This practical background led to his first experiments with computers – like all children, his interest lay in games: ‘My first brush with real programming was through games, when I was eleven or twelve. I liked the loader screens the games put up, so wrote a program to capture them, copy them to memory, and display a section by pressing a key.’

### Telecom Skills

School led to The Queen’s College at Oxford University, where he pursued doctoral research in semiconductor physics. During his studies, he ran into his first computer virus, Spanish_Telecom, which he disassembled.

He recalls a misguided statement he made at the time, to the effect that anti-virus ‘guys’ probably wrote a lot of viruses themselves: this made its way to a director of *Virus Bulletin*, and led to Ford visiting *VB* to ‘get the real story’. The rest, as they say, is history – one of Ford’s first articles for *VB* was an analysis of Spanish_Telecom: ‘I did a little writing, a lot of reading, and eventually became Editor.’

‘And what a day my first one was!’ he recalled. ‘It was the *VB* conference in Edinburgh. Being dropped in the middle of some of the best anti-virus people in the world was going in at the deep end. I spent my time absorbing knowledge, and watching. It was a great introduction.’

Ford left *VB* in May 1995 to become Director of Research at the *NCSA*: ‘*NCSA* was an exciting opportunity for me, as I had worked a lot on testing in my research, and revamping their certification scheme was an interesting project. However, after Sarah [*Gordon*] and I were married, living together and having a good work as well as personal relationship was vital.’

After a spell with *Command Software*, where his wife was also working, Ford believes he has found the right combination at *IBM*: ‘The technology employed by *IBM AntiVirus* is truly cutting edge, and the atmosphere in the Research Labs is second to none. I really think that we’ve found our home!

‘At *VB*, I learned about the industry. At *NCSA*, I used that knowledge to put together the certification scheme. At *Command*, I worked on QA, virus analysis, and trouble-shooting on various platforms. Now, at *IBM*, I’m implementing things I’ve been working on; working on things I only dreamed about. We’re currently developing a computer immune system, an automated way of dealing with new viruses. When that is complete, we’ll be looking at an entire paradigm shift in terms of what virus protection really means.’

### Trends and Techniques

Polymorphism is, for Ford, of interest to scanner manufacturers only; irrelevant in the ‘big picture’. He sees the bigger problem as polymorphics which attempt to hide their entry point, but feels macro viruses are another matter altogether: ‘They reflect a trend within an increasingly *Windows*-based community. We’ve separated user and computer by hiding a lot of the interaction behind a point-and-click interface.

‘That’s good, in that the software is easier to use; you needn’t know what’s going on beneath the surface. However, most users don’t know the real effect of double-clicking on an icon. Does it run a program? Does it split up an archive? Is it a link to a program stored elsewhere? They don’t know, which makes it difficult for them to decide if the action carries a risk.

‘Furthermore, developers add continually to the power of application software, often without considering the security impact. The macro problem will continue to get worse, until application developers start thinking about the ways in which their new features could be abused, not just used.’

As for heuristics, they are in Ford’s opinion useful but not omnipotent; simply another weapon in the battle: ‘A good heuristic analyser should produce few false positives, as these can make it unusable. Further, 100% detection cannot be expected from products using only such techniques.’

He views integrity checkers as effective and extremely underused, but sees a problem in the amount of work involved in interpreting their results. ‘There is a raft of other “generic” techniques,’ he continued. ‘It would be unwise to limit ourselves to scanners, although I think they will be the most powerful part of our arsenal for the foreseeable future.’

Until recently, received wisdom held that it would be almost impossible to create a new anti-virus product from scratch, due to ever-increasing numbers of viruses. Now, according to Ford, the advent of macro viruses has allowed a niche market to be created, but even there, creating a new scanner would be a heavy task.

‘There are already products which deal only with macro or *Windows* viruses. Whether or not such products flourish depends on how well traditional anti-virus products deal with the problem. Like nature, commerce abhors a vacuum: if products leave gaps in protection, someone will try and fill them. This is good: competition breeds competence. Many people feel that an anti-virus industry with only two or three main players would be bad for users.’

The Richard and Sarah show played to enthralled audiences.

### Best Foot Forward

And the virus writers? Ford believes legislation will never prevent people writing viruses: ‘If you’re smart, you’ll never get caught. Who wrote Concept? Who wrote Laroux? The best road forward is probably education. We send mixed messages about right and wrong; I still see articles telling us virus writers are unsung heroes pushing computing’s limits.’

As Ford put it: ‘If professional computer users can’t make up their minds whether virus writing is right or wrong, what chance does a sixteen-year-old have?’

Although he has never written a virus himself, Ford has had contact with several (‘mostly ex-’) virus writers: ‘Mostly, they’ve been intelligent and interesting. Virus writing to them seems a kind of aberration, something they can’t quite see as wrong. I’ve spoken to Dark Avenger a couple of times, which was interesting – he’s clever with words.

‘To an extent, I understand the fascination for virus writers. Somehow, though, they don’t seem able to acknowledge the harm they can cause. The problem is bad enough without adding to it by carelessness. Even when examining virus-writing tools, you have to ensure that everything you do is done in a secure environment which can be completely erased when you are done. It is easy to create a new virus variant by accident, just single-stepping through a sample with debug.’

### Where Do You Go To…

At 29 years of age, Ford has a long working life ahead. Does he see himself staying in the anti-virus arena? ‘The computer industry is such a fast-changing world that it’s foolish to ignore the possibility of changes in direction. The Internet, in particular the WWW, will change many of the ways in which we view traditional computer security problems, as will users’ increased distance from the actual operation of their computers – this is not, I believe, a good thing.

‘It’s that rapid change which makes working at TJ Watson so exciting. The entire lab is filled with “next generation” technology, in the process of being applied today!’

Ford intends to keep his skills as diverse as possible, having gone from physicist to anti-virus researcher through programmer, writer, and tester. The issue of virus protection, in his view, is a large one; so large, and covering so many platforms, that it would be easy to lose sight of the whole by concentrating on the detail.

### A Double Life

Ford’s life, both professional and personal, has changed dramatically in the past two years, from a bachelor existence in a sleepy English town, working day and night to get *Virus Bulletin* to print, to a happily-married man working for a well-known anti-virus developer. It was through *VB* that Ford first met Sarah Gordon…

‘The first time I spoke to Sarah was after I wrote something about her in *VB* which she took offence to. As she was in the UK at the time, I asked her if she would like to have lunch and discuss it… but I never called her back :-).’

Their next meeting was at the *VB* Conference in Jersey, in 1994. Ford admits to arranging to meet up with her in the hope that he could persuade her to write some articles for *VB*: ‘From the first time I saw her there,’ he recalls, ‘I wanted to know Sarah. I sat opposite her for dinner one night, and frankly I can’t remember anyone else who was there.’

The two met again at the EICAR conference in 1994: ‘My fate was sealed,’ Ford grins. ‘From then on, I pursued her relentlessly, moving half-way across the world to court her.’

Their engagement was announced at *VB 95*, and they married in Balquhidder Kirk, Scotland, on 4 December 1995: ‘We’re working at the happily-ever-after bit now.’

Ford confesses that being married to another anti-virus researcher has altered his perspective. The two see their working habits reflected in each other, and try to make more space for each other: ‘If anything,’ he said, ‘life is more balanced, not less. Workwise, it can be tough. Sarah has a unique perspective on things, so it can be tricky when we disagree, as neither of us is ever wrong :) .

‘Working at the same company accentuates this, but it’s nice to work with someone you know really well – I have complete trust in her. We bounce a lot of ideas off each other – we have different strengths and weaknesses, so working together is very effective.’

Moving to the USA was more of a surprise than Ford had anticipated: ‘It was a culture shock. It’s stronger than if you move somewhere where you know it’s going to be different. Here, I keep thinking we speak the same language and have the same customs, though we don’t. The differences are more subtle, and thus easier to overlook. My main problem is ordering fast food on a drive-through. Two years later, I’m still trying to find out how to get what I actually want!’

Despite this, Ford is entirely content with his life. Doubtless within the next year or two, some other challenge will arise that he will tackle with the same gusto with which he approaches everything he has faced thus far – and doubtless this will only add to his contentment.

# VIRUS ANALYSIS

## Silicon Implants

*Igor Muttik*
*Dr Solomon's Software Ltd*

In February this year, I received some files which had been downloaded from an Internet virus exchange site and forwarded to us for analysis. 'Ah, the usual rubbish…', I thought; for it is rare to get new (let alone interesting!) viruses from such sources – if a file is not already identified as containing a known virus, it is usually either a corrupted virus, or not a virus at all. It looked as though this would again be the case, but then, amongst these files, I came across a new virus – Implant.6128.

Implant is unusual in many aspects – it has full stealth, and is both polymorphic and multi-partite. Stranger still, it works reliably – I have never seen a virus so complex and yet so stable. After all, it is both well known and intuitively obvious that as software gets more complex, it has more bugs.

In my opinion, this explains perfectly why primitive computer viruses (most boot sector and macro infectors) are the most common in the wild. Sophisticated viruses have more bugs, and thus have a smaller chance of surviving unnoticed in the field. Implant is a rare exception to this general rule.

Returning to the virus' specifics, it is extremely polymorphic – the complexity of its decryptor by far exceeds that of many other famous polymorphic viruses. It is also extremely multi-partite, infecting COM, EXE and SYS files as well as the hard disk MBR and floppy boot sectors.

Finally, Implant makes it impossible to boot the computer from a clean DOS system diskette: it does this using the circular extended partition technique, first seen implemented in Rainbow [*see VB, September 1995, p.12*].

### Initial Infection

When an infected file is run, or the infected floppy is left in the A: drive at boot time, the virus takes control in the traditional manner. After it decrypts itself, it checks the processor type: if the computer is 8088- or 80286-based (i.e. is an XT or an AT), Implant immediately infects another file. However, if the machine is an 80386 or above, the virus issues its 'Are you there?' call – Int 12h, CX=029Ah, SI=0BADh, DI=FACEh.

If, on return from the call, the SI and DI registers are set to DEADh and BABEh respectively (I wonder how many other words can be squeezed into 16 bits?) the virus assumes it is already active and proceeds to infect a file. Otherwise (if it is not already resident), it creates an array of 1024 random bytes (which will later be used by the virus' polymorphic engine) and passes control to the hard disk infection routine.

This routine copies the MBR to sector 3 on track 0, and then finds the active partition record in the partition table, checking whether it is a 16-bit FAT DOS system (that is, the type field is set to 4 or 6).

If so, Implant removes the active flag, sets the partition type to 5 (Extended DOS partition) and makes the pointer to its first sector point to the MBR (creating a so-called 'circular extended partition').

Then the virus analyses the code in the MBR: it follows the jump chain (if present), and puts its code at the destination of the final jump – the virus code is such that it needs to leave only 35 bytes in the MBR! Implant next writes the MBR back to disk by direct manipulation of I/O ports (this will make it compatible with IDE and MFM drives, but not SCSI).

After the write attempt, the virus rereads the MBR and checks whether the checksum of what was read matches what was written. If not, the virus gives up, and passes control to the host program.

Then the virus writes its body into 12 sectors on track 0 starting at sector 4, right after the saved MBR. Implant does not forget to check whether there is sufficient space on track 0 – if there are fewer than 13 sectors before the start of an active partition, the virus will not infect the hard drive, nor modify anything on track 0.

Implant does not recognize itself in the MBR. It just checks whether a resident copy is already present using its 'Are you there?' call. If it is not in memory, it loads the MBR and scans for an active partition. An already-infected MBR will not have this, so the infection will fail at this point – there is no risk of multiple infection.

There are two main branches in the virus code. If the virus is run from a file (COM, EXE or SYS), control transfers to the host and nothing is left resident in memory. If, however, the virus is run from a boot sector (either that of a floppy or the hard disk's MBR), it seizes 7KB of DOS memory (by the familiar technique of reducing the word at memory offset [0:413h]), copies itself to the newly-created hole in memory just beneath the top of conventional memory, and intercepts some system interrupts.

The method by which the virus infects the hard drive means that an *MS-DOS* system floppy cannot be used to clean-boot an Implant-infected PC. The circular extended partition will make *MS-DOS v5* onwards, *Novell DOS 7*, and *DR-DOS 6* hang. Fortunately, it is still possible to use versions 3.30 or 4.0 of *MS-DOS*, or *PC-DOS 5* and *6*, which will boot without problem. After booting, however, drive C will still, of course, be inaccessible: attempts to access this drive will result in the error 'Invalid drive specification'.

### Booting the Infected System

When booting, the virus hooks interrupts 12h (self-recognition and stealth), 13h (disk I/O; for stealth and to infect floppies), and 1Ch (timer; to intercept DOS interrupts later on). All three are used to intercept Int 21h: the virus can do this in three ways:

- thirty seconds after the computer is booted (checked using Int 1Ch)
- when an infected program is run: when such a program issues the 'Are you there?' Int 12h call (see above) the resident copy of a virus will immediately hook Int 21h
- when a program attempts to write to disk using Int 13h

The virus has specific knowledge of some versions of DOS, and tries to get the real DOS entry point by following the jumps and doing some checks. If an attempt to get the real entry point fails, the virus simply uses the one taken from the Interrupt Vector Table.

When the virus has hooked Int 21h, it monitors the following DOS functions: 2Ah (Get date; used in a payload), 4B00h (Exec), 3Eh (Close), 43h (Attribute), 56h (Rename/Move), 4Ch (Terminate), 3Dh (Open), 6Ch (Open/Create), 11h/12h (Findfirst/Findnext FCB), 4Eh/4Fh (Findfirst/Findnext), 3Fh (Read), 4B01h (Load), 40h (Write), 5700h (Get timestamp), 5701h (Set timestamp). These functions are used to infect files and conceal infection (full stealth).

During infection, the virus also intercepts Int 24h (Critical error handler) to suppress error messages.

### Infection of Files

The virus infects files as they are run or opened. However, if any infected files are copied to diskette, the files on the diskette will be clean (despite the fact that the diskette's boot sector is infected) – Implant is 'full stealth'. Running the file from the floppy does not infect it either. How, then, are infected files passed between users?

The first thing the virus checks when any program calls any monitored DOS function is the program's name, paying special attention to files named AR*.*, PK*.*, LH*.*, and BA*.* (archiving utilities; specifically, ARJ, PKZIP, LHA and BACKUP). This information is used to turn off stealth mode when any of these archivers is executed. Thus, the virus ensures all executable files are packed into archives and backups are infected, whether on floppy or hard disk.

Further, it will not infect files called TB*.*, SC*.*, F-*.*, GU*.*, nor those containing the letters V, MO, IO, DO, IB or the digits 0-9. Thus the virus avoids a wide variety of anti-virus programs, DOS system files, and goat files used by virus researchers (which usually have digits in the name).

Implant infects only files with the extensions COM, EXE and SYS. COM and SYS files longer than 52801 bytes are not infected. Files with time-stamps set to 62 seconds are assumed already infected – this is the virus' infection stamp. To check whether a file is an EXE file, the virus adds the first two bytes of the file (for an EXE file, 4D5A or 5A4D) together: if the sum is A7h (A7h=4Dh+5Ah), the file is assumed to have an EXE header. Simple and elegant.

When resident, Implant denies access to files named CHKLIS*.*. These patterns match CHKLIST.MS or CHKLIST.CPS, and prevent *Microsoft's* and *Central Point's* scanners from working properly.

If WIN.COM is executed, the virus adds a parameter /D:F to the program's command-line. This argument turns off *Windows'* 32-bit disk access, which enables infection of floppies accessed from within *Windows*. If TBSCAN is executed, the virus adds the command-line parameters 'co' and 'nm', which instruct the program to skip the memory check and not use direct disk access ('compatibility mode').

### Infection of Floppies

The floppy disk boot sector is infected in much the same manner as the MBR. The virus follows the jump chain in the floppy boot sector and writes 35 bytes of its code there. The encrypted polymorphic virus body is placed on a floppy on an additional track (number 80) which it first formats. This track will have 13 sectors: the first will carry a copy of an original boot sector; the rest will be occupied by the encrypted virus body. To infect floppy disks, Implant uses Int 40h, which usually points to BIOS code.

> *"this virus ... shows that Griyo uses approaches that are neither common nor trivial"*

The virus infects only 1.2MB or 1.44MB floppies. It checks the total amount of sectors on the media (the word at offset 13h in the boot sector) and proceeds with infection only if the number of sectors is B40h or 960h (2880 or 2400, respectively). For self-recognition, the virus checks the two letters at offset 21h from the last jump in the chain (if any): all infected floppies contain the marker 'CR' at this point.

There is a bug in floppy infection: if the boot sector starts with a JMP (opcode E9h, not usual EBh), the virus code is inserted 1 byte lower than necessary. Still, the virus is able to work as the first instruction of its code is CLI, which takes just 1 byte and is not absolutely necessary.

### Polymorphic Engine

Implant's polymorphic engine is very powerful. Suffice it to say that it supports subroutines, conditional jumps with non-zero displacement, and memory writes. This engine takes a good half of the virus' code.

The engine makes extensive use of the table of random bytes created during the initialization phase. The approach of using a table generated just once during the installation of the virus into memory classifies Implant as a slow polymorphic. This means that the variety of the polymorphic decryptors is artificially limited until the next reboot of the PC. It poses some problems for anti-virus researchers, as it becomes difficult to create enough files infected in enough different ways to test detection.

Files are encrypted in two layers: the first is polymorphic; the second is simple XOR encryption with a slightly variable decryptor. Some attempts are made to prevent tracing the second decryptor, but no anti-emulation tricks are used.

### Stealth Properties

Implant stealths its modifications to the MBR and FBR. The virus also does not allow writes to the sectors on track 0 which are used by the MBR copy and the virus body (sectors 03h to 0Fh).

If any of the programs ME*.*, CH*.*, SY*.*, SM*.* is run (these patterns appear to be intended to match MEM, CHKDSK, SYSINFO and SMAP) the virus spoofs the value returned by Int 12h (free RAM) by adding 7K to the real figure. Hence, the amount of memory is reported as it was before infection.

The stealthing of infected files is more sophisticated than that of the MBR and floppy boot sector. Most modern stealth viruses do ‘semi-stealth’ (just the change in the file size is concealed). Implant, on the other hand, is full stealth, so when the virus is active, even integrity checking programs will not report any file modifications.

A common problem to all stealth viruses is how to suppress error messages from the CHKDSK utility. When run on a system infected with a stealth virus, CHKDSK reports allocation errors, because reported file sizes do not match their actual sizes (i.e. the reported size in bytes does not match the number of clusters in the file allocation table). Implant recognizes that CHKDSK.EXE (or a similar utility) is being run, and turns off its stealth routine whilst the disk check is performed.

If there is any doubt as to whether or not a PC is infected by Implant, the easiest way to check is to create a file called CHKLIST. If there are problems accessing this file, the virus is almost certainly resident. To check if a particular executable is infected, it is probably easiest to pack the file into an archive and check whether the size inside is the same as outside. If not, the file is infected.

### Payload

Implant’s payload triggers on 4 June, after any program asks for the system date. The payload is buggy: it was apparently supposed to destroy the contents of track 0, rendering the system unusable, but the virus itself rejects the attempt to overwrite the infected MBR! So, the destructive part of the payload does not work.

After this unsuccessful attempt to zap itself, the virus slowly types the following text in the middle of the screen (green letters on a black background, accompanied by a rattling, perhaps meant to resemble the noise of a typewriter):

```
<<< SuckSexee Automated Intruder >>>
Viral Implant Bio-Coded by Griyo/29A
```

Then the PC freezes. After a reboot (until you change the CMOS clock setting) the payload will eventually trigger again because some program, sooner or later, will try to get the system date – and the cycle will begin again…

### Summary

Implant impressed me. It is definitely written by a talented person – it is a pity his skills are used so destructively. I recently received another interesting virus (Gollum.7167) from the same author (carrying the signature ‘Griyo/29A’): it spreads via infected standard DOS EXE files which drop a VxD in *Windows’* SYSTEM directory (called GOLLUM.386) and registers it in SYSTEM.INI. When *Windows* is started, the VxD becomes active and will infect DOS EXE files run in the DOS box. This virus again shows that Griyo uses approaches that are neither common nor trivial.

I wonder if this is talent comparable to the Dark Avenger or the author of One_Half? I sincerely hope such a gifted person will find better things to do than write viruses.

## Implant.6128

| | |
|---|---|
| Aliases: | Implant.mp.6128. |
| Type: | Resident, full stealth, polymorphic, multi-partite. |
| Infection: | COM, EXE, SYS, MBR, FBR. |
| Recognition: | Try to create and access file named CHKLIST (difficulty in accessing the file indicates that the virus is active) |
| Self-recognition: | 62 seconds marker in files, ‘CR’ signature on floppies. No self-recognition in the MBR (see text). |
| Hex Pattern in Files: | None possible |
| Hex Pattern on Disks: | 02BB 007E B9?? ??2A F6CD 1372<br>0306 53CB CD18 4352 |
| Hex Pattern in Memory: | B99A 02CD 1281 FEAD DE75 0B81<br>FFBE BA75 05EB 00E9 |
| Payload: | Displays text and hangs PC on 4 June. |
| Removal: | Recover affected files from a backup or replace with originals. |

# COMPARATIVE REVIEW

## Looking out Windows (95)

Just under a year ago, *Virus Bulletin* carried out its first comparative review of *Windows 95* anti-virus products. At that time, *Windows 95* was nearly a year old, and in many ways it was still fairly new, and not very well understood. Times have changed.

*Windows 95* is now for many companies the client operating system of choice: as time goes on, and new PCs are gradually bought and slowly eclipse the old ones, *Windows 95* gains more of a foothold over its 16-bit, 640K-memory-limited, predecessor. The expected rise in *Windows NT* is happening, but *95*, with its smaller memory and hardware requirements, is beginning to rule the roost, at least on network clients.

### Testing, One Two Three

Sixteen products took part in the review of June 1996: this time, the number has increased to twenty-one. Many things remain unchanged from the last review; for example, it is not a requirement that submitted products be ‘proper’ *Windows 95* applications (i.e. be a 32-bit PE executable). It must simply be that company’s solution for a PC running *95*.

Many of the tests also remain similar to those of last year. For example, there are still four test-sets (In the Wild Boot, In the Wild File, Standard, and Polymorphic). All have grown since the last comparative – file infectors are now stored on CD to make it easier to guarantee that no product has modified any of them. Speed tests are still performed over three media: an uninfected diskette (43 COM+EXE files; 997,023 bytes), an infected diskette (the same 43 COM+EXE files infected with Natas.4744; 1,201,015 bytes), and a clean hard drive (5,500 COM+EXE files spread over 121 directories; 546,932,175 bytes). This final test serves double duty, acting also as a false positive test.

The numbers of viruses and samples in the test-sets has increased – readers are referred to the final page of the review for figures in this area. Also at the end is a URL for a document describing the procedure for calculating the detection percentages.

### New Tests

One significant new range of tests has been added: this time we tested the performance of the on-access component of the various products. The phrase ‘on-access component’ refers to the part of the product that stays memory-resident on the computer watching for viruses as the user works – it is this part of the product which is most relied upon by most users for the bulk of the virus protection. *Virus Bulletin* knows of no published test which goes into this level of detail concerning this aspect of the products.

One aspect of the tests as currently performed is that infected files are not actually *run*. The tests measure the ability of the resident protection systems to detect viruses in files as they are *copied*. This gives a legitimate measure of a product’s detection abilities, while keeping large-scale automated testing possible.

### Technical Notes

The same machine was used throughout (technical specifications are given at the end of the review): this reliance on one machine is necessary in order that the speed figures should mean anything. For each product, a clean installation of *Windows 95* was used to ensure a level playing field – a sector-level image of the hard disk was used to allow speedy and unattended reinstallation of the operating system.

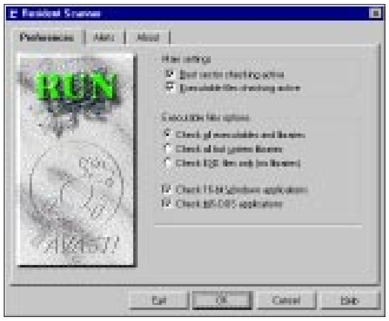
The computer used (a Pentium 90) is now slightly below ‘entry-level’; however, it has 80MB RAM, a figure far above entry-level. This helps minimize paging, and in some ways helps make up for the slowish processor.

The number of boot sector viruses is now 88. Coupled with the two types of scan test (on-demand, on-access) and the twenty-one participating products, this is enough to give the most determined and flexible reviewer a severe case of RSI.

## Alwil AVAST! v7.50-16

In previous reviews, *Alwil’s AVAST!* has performed extremely well – readers will recall that in the January DOS review it missed a mere four virus samples. Its In the Wild detection rate is slightly down since that review: for some reason that this reviewer was unable to work out, it seemed to miss rather a lot of boot sector viruses (ten of the 88 were not detected. Aside from this problem, the product performed admirably in all on-demand tests.

However, the on-access component of the product is unable to check files as they are opened; only as they are executed. This causes problems with macro viruses: when an infected document is opened by *Word*, *AVAST!* does not detect that document as infected. The developers inform *Virus Bulletin* that the next version of the resident software will solve this problem. It was thus impossible to test the on-access component against file infectors: it was, however, tested against the boot sector test-set, where it produced a higher rate of detection than the on-demand scanner!



Main settings

☑ Boot sector checking active

☑ Executable files checking active

Executable files options

● Check all executables and libraries

○ Check all but system libraries

○ Check EXE files only (no libraries)

☑ Check 16-bit Windows applications

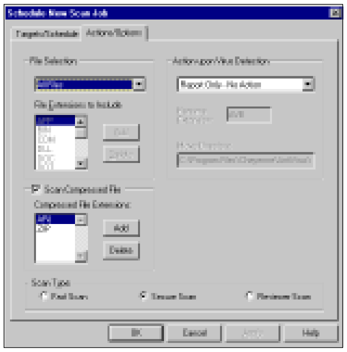
☑ Check MS-DOS applications

In terms of the other tests, there is nothing remarkable to say. *AVAST!* is the second-slowest scanner when tested against the clean hard drive, but it suffered no false positives, nor other obvious problems.

The interface is much the same as it was a year ago – idiosyncratic, but perfectly usable. The product's biggest omission at the moment is the inability of the on-access component to check files as they are opened.

## Cheyenne InocuLAN v4.0; 03.32

*Cheyenne's* In the Wild detection rate continues to improve: up from almost 94% in the January DOS comparative to over 99% today, missing only Goldbug and Ornate. This is an impressive performance from the often under-regarded *InocuLAN*, placing it reasonably near the top of the heap in this area. Detection in the Standard and Polymorphic sets is also admirable.



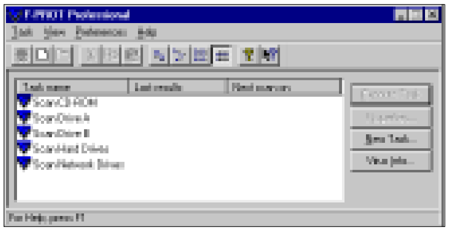
In other areas, on-access detection is fractionally lower than on-demand – the difference is three polymorphic samples. It appeared at first, and until the last test-set, that the detection rate was going to be the same.

In terms of usability, *Cheyenne's* products have always been up there with the best of them, and their *Windows 95* product is no exception. It is very easy to manipulate the program's many options, although it is not obvious what some of the icons on the main screen do. However, the expected tool-tips alleviate this problem.

## Command F-PROT Professional v2.25

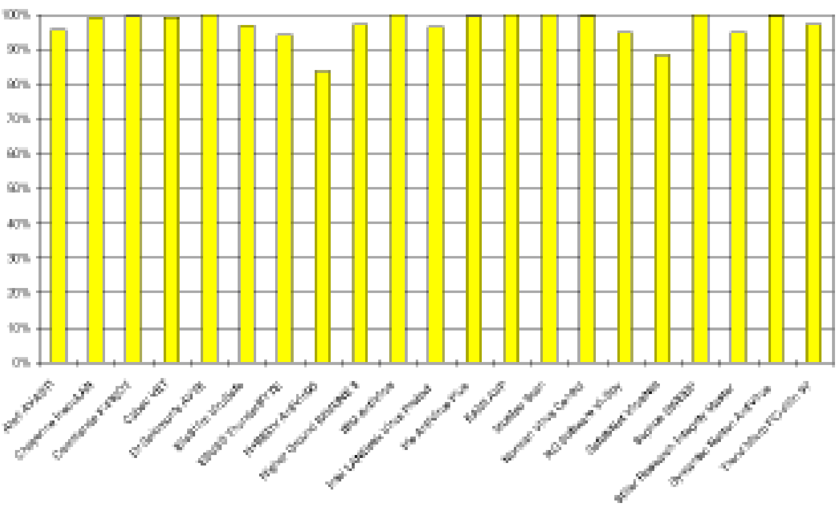
A year ago, we remarked that this product has an exceptionally nice interface: this remains the case; it is still one of the least cluttered and æsthetically pleasing of the products tested.

Its In the Wild score is also pleasing, missing only the three samples of Plagiarist.2051. In the other sets, things are less good: the Polymorphic score is, as in all reviews for the past two years or so, a weak spot. The now-almost-mythical version 3 is said to fix this, and is also said to be close to release. But then, we first heard that about 18 months ago… In other areas, the product fares well. It is fairly fast, and encountered no false positives. Still, roll on the new version!



Scan CD-ROM
Scan Drive A
Scan Drive B
Scan Hard Drives
Scan Network Drives

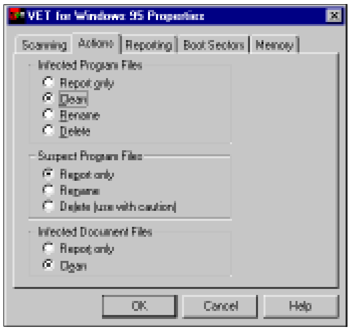
Results Against the In the Wild Test-set (On-demand)



## Cybec VET v9.3.1

There was significant difference between the detection rates of *Cybec's* on-demand and on-access components: for some reason, the memory-resident portion did not do as well as the other on the boot sector test-set. Aside from this, however, detection was well above average (breaking the 99% barrier in the In the Wild Overall category).

In terms of speed, *VET* is always one of the ones to beat. In this test, it is only beaten by *IBM AntiVirus'* second scan: clocking in at more than 3MB/second on the false positive test is very impressive for a *Windows 95* product. As expected, it encountered no false positives.



Infected Program Files
○ Report only
● Clean
○ Rename
○ Delete

Suspect Program Files
● Report only
○ Rename
○ Delete (use with caution)

Infected Document Files
○ Report only
● Clean

*VET for Windows 95* has an interface perhaps best described as 'different from the rest'. It was more difficult to get used to than some of the other products under test, but, as with most, it starts to make sense once you're into the swing of it.

## Dr Solomon's AVTK v7.69

Alphabetically the first of the five products to score 100% on the In the Wild Overall category with its on-demand scanner, *Dr Solomon's AVTK* ranks joint first (with *Sophos*

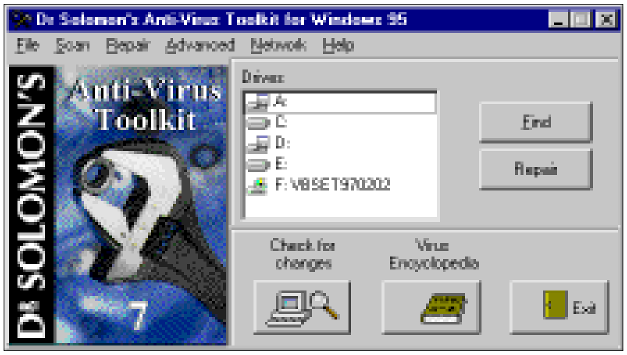
## Results Against the In the Wild Test-set (On-demand)

| | ItW Boot | | ItW File | | ItW Overall | Standard | | Polymorphic | |
|---|---|---|---|---|---|---|---|---|---|
| | Number | Percent | Number | Percent | Percent | Number | Percent | Number | Percent |
| Alwil AVAST! | 78 | 88.6% | 509 | 100.0% | 95.7% | 765 | 100.0% | 11500 | 95.8% |
| Cheyenne InocuLAN | 87 | 98.9% | 506 | 99.3% | 99.1% | 759 | 99.3% | 11366 | 90.8% |
| Command F-PROT | 88 | 100.0% | 506 | 99.3% | 99.6% | 614 | 87.1% | 7060 | 53.5% |
| Cybec VET | 87 | 98.9% | 505 | 99.3% | 99.1% | 628 | 88.1% | 11500 | 95.8% |
| Dr Solomon's AVTK | 88 | 100.0% | 509 | 100.0% | 100.0% | 763 | 99.7% | 12000 | 100.0% |
| EliaShim ViruSafe | 82 | 93.2% | 502 | 99.5% | 97.1% | 492 | 76.5% | 9441 | 71.5% |
| ESaSS ThunderBYTE | 85 | 96.6% | 470 | 92.8% | 94.2% | 602 | 85.3% | 7611 | 58.0% |
| H+BEDV AntiVir/95 | 60 | 68.2% | 474 | 93.5% | 83.8% | 606 | 86.4% | 8393 | 67.0% |
| Higher Ground IMMUNE II | 83 | 94.3% | 505 | 99.1% | 97.3% | 453 | 71.2% | 10883 | 88.9% |
| IBM AntiVirus | 88 | 100.0% | 509 | 100.0% | 100.0% | 764 | 99.7% | 11500 | 95.8% |
| Intel LANDesk Virus Protect | 83 | 94.3% | 497 | 97.7% | 96.4% | 458 | 71.4% | 10882 | 87.8% |
| Iris AntiVirus Plus | 87 | 98.9% | 509 | 100.0% | 99.6% | 759 | 99.3% | 11419 | 91.2% |
| KAMI AVP | 88 | 100.0% | 509 | 100.0% | 100.0% | 691 | 93.4% | 11500 | 95.8% |
| McAfee Scan | 88 | 100.0% | 509 | 100.0% | 100.0% | 732 | 97.5% | 12000 | 100.0% |
| Norman Virus Control | 88 | 100.0% | 508 | 99.6% | 99.8% | 642 | 90.6% | 11318 | 92.6% |
| RG Software Vi-Spy | 86 | 97.7% | 475 | 93.3% | 95.0% | 588 | 84.1% | 7832 | 59.4% |
| SafetyNet VirusNet | 84 | 95.5% | 418 | 83.8% | 88.3% | 670 | 91.3% | 7050 | 54.5% |
| Sophos SWEEP | 88 | 100.0% | 509 | 100.0% | 100.0% | 763 | 99.7% | 12000 | 100.0% |
| Stiller Research Integrity Master | 84 | 95.5% | 475 | 94.7% | 95.0% | 573 | 81.3% | 4082 | 28.6% |
| Symantec Norton AntiVirus | 88 | 100.0% | 508 | 99.6% | 99.8% | 565 | 82.4% | 10500 | 87.5% |
| Trend Micro PC-cillin 97 | 83 | 94.3% | 505 | 99.1% | 97.3% | 469 | 72.8% | 10883 | 88.9% |

*SWEEP*) in the other test-sets as well. In the whole test it missed two samples with the on-demand scanner (both Midin.765), and three with the on-access component (the two Midins again, and one sample of Cruncher).

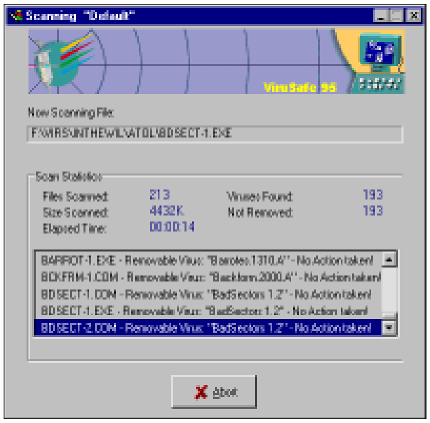
The product clocks in towards the upper end of the rankings on clean files, and at the bottom on the less important infected files test. There were no false positives.

The product's interface owes little to *Windows 95*, and is clearly a straight port of the *Windows 3.1* version. This has both its good and its bad points: on the plus side, it is very easy for upgrading users to use the new version (and it's easy to produce the new version!). On the minus side, however, it does not take advantage of any of the interface improvements which *Windows 95* offers to the developer.



## EliaShim ViruSafe v05/02/97

What has happened to *ViruSafe*? The somewhat dowdy interface reviewed last year has been replaced by a new, more visually-thrilling one, with colourful animations and icons vying for your attention.



Now Scanning File: F:\VIRS\INTHEWIL\ATOL\BDSECT-1.EXE

Files Scanned: 213 Viruses Found: 193
Size Scanned: 4432K Not Removed: 193
Elapsed Time: 00:00:14

```
BARROT-1.EXE - Removable Virus: "Barrotes.1310.A" - No Action taken!
BCKFRM-1.COM - Removable Virus: "Backform.2000.A" - No Action taken!
BDSECT-1.COM - Removable Virus: "BadSectors 1.2" - No Action taken!
BDSECT-1.EXE - Removable Virus: "BadSectors 1.2" - No Action taken!
BDSECT-2.COM - Removable Virus: "BadSectors 1.2" - No Action taken!
```

## Results Against the In the Wild Test-set (On-access)

| | ItW Boot | | ItW File | | ItW Overall | Standard | | Polymorphic | |
|---|---|---|---|---|---|---|---|---|---|
| | Number | Percent | Number | Percent | Percent | Number | Percent | Number | Percent |
| Alwil AVAST! | 85 | 96.6% | n/a | n/a | n/a | n/a | na/ | n/a | n/a |
| Cheyenne InocuLAN | 87 | 98.9% | 506 | 99.3% | 99.1% | 759 | 99.3% | 11363 | 89.8% |
| Command F-PROT | 88 | 100.0% | 503 | 98.6% | 99.1% | 609 | 86.8% | 7060 | 53.5% |
| Cybec VET | 79 | 89.8% | 505 | 99.3% | 95.7% | 628 | 88.1% | 11498 | 93.7% |
| Dr Solomon's AVTK | 88 | 100.0% | 509 | 100.0% | 100.0% | 762 | 99.5% | 12000 | 100.0% |
| EliaShim ViruSafe | 83 | 94.3% | 499 | 98.7% | 97.1% | 492 | 76.5% | 9440 | 71.5% |
| ESaSS ThunderBYTE | 83 | 94.3% | 480 | 94.4% | 94.4% | 668 | 91.2% | 8409 | 63.0% |
| H+BEDV AntiVir/95 | 0 | 0.0% | 474 | 93.5% | 57.8% | 606 | 86.4% | 8394 | 68.1% |
| Higher Ground IMMUNE II | 83 | 94.3% | 505 | 99.1% | 97.3% | 453 | 71.2% | 10883 | 88.9% |
| IBM AntiVirus | 61 | 69.3% | - | - | - | - | - | - | - |
| Intel LANDesk Virus Protect | 0 | 0.0% | 491 | 96.6% | 59.7% | 458 | 71.2% | 10642 | 83.2% |
| Iris AntiVirus Plus | 85 | 96.6% | 509 | 100.0% | 98.7% | 759 | 99.3% | 11924 | 96.4% |
| KAMI AVP | n/a | n/a | n/a | n/a | n/a | n /a | n/a | n/a | n/a |
| McAfee Scan | 87 | 98.9% | 507 | 99.5% | 99.3% | 731 | 97.4% | 11345 | 90.7% |
| Norman Virus Control | 84 | 95.5% | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| RG Software Vi-Spy | 85 | 96.6% | 474 | 93.2% | 94.5% | 588 | 84.1% | 7832 | 59.4% |
| SafetyNet VirusNet | 87 | 98.9% | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| Sophos SWEEP | 88 | 100.0% | 509 | 100.0% | 100.0% | 763 | 99.7% | 12000 | 100.0% |
| Stiller Research Integrity Master | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| Symantec Norton AntiVirus | 88 | 100.0% | 508 | 99.6% | 99.8% | 565 | 82.4% | 10500 | 87.5% |
| Trend Micro PC-cillin 97 | 83 | 94.3% | 505 | 99.1% | 97.3% | 459 | 71.5% | 10883 | 88.9% |

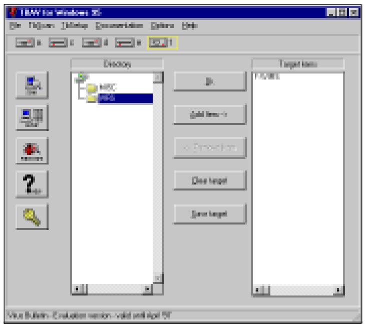
As for detection, that too is rising. In the Wild detection is up on a year ago, and the Polymorphic rate has more than doubled! Admittedly, it is still relatively low at 71.5%, but who knows what will come next?

On the down side, the on-access component was unable to detect any viruses in files accessed from the test-machine's CD drive. When the files were copied to the hard drive and the test performed again, they were detected, so clearly there are some compatibility issues to be ironed out. Otherwise, the on-access scanner produced almost exactly the same detection rate as the on-demand one.

Overall, this product is coming along quickly, and *VB* looks forward to seeing it again in a few months time.

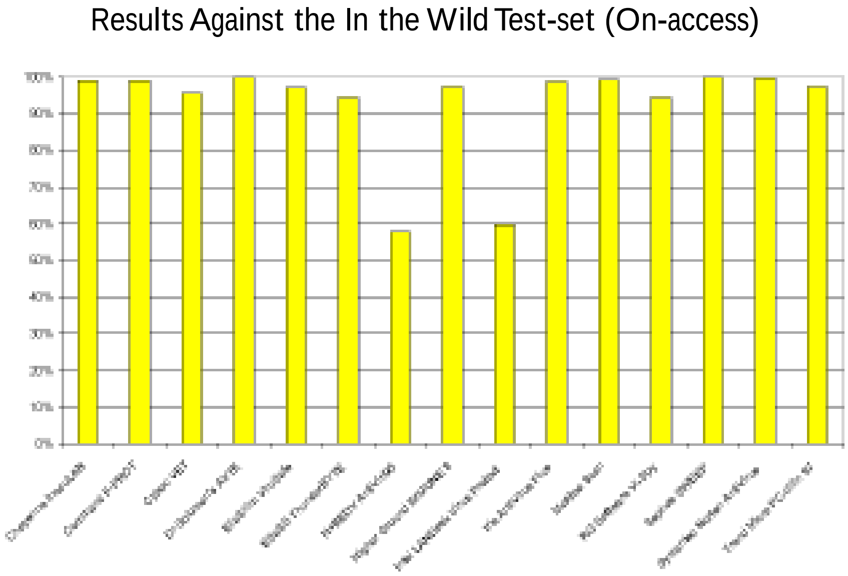
## ESaSS ThunderBYTE v7.07

What's the matter with this version of *ThunderBYTE*? It can only be assumed that there's some sort of problem, as detection rates are much lower than we have come to expect. 58% in the Polymorphic set? Surely not! Whatever happened in this release has also had a significant effect in the other sets: 94.2% in In the Wild Overall? Further, the on-access component performs better in all areas. Curiouser and curiouser…


TBAV for Windows 95
File TbScan TbSetup Documentation Options Help
Directory
Target items
MISC
Add items ->
Clear target
Save target
Virus Bulletin - Evaluation version - valid until April '97

The fact remains, though, that in this review *ThunderBYTE* performs relatively poorly in terms of detection. In the speed tests, it does considerably better (it is the proud owner of the third highest point on the hard drive graph).

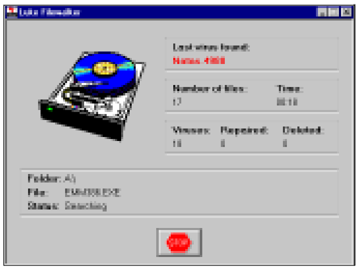
*ThunderBYTE's* interface is simple to use, and the product offers all the expected functionality in a nicely put-together overall package. Hopefully, whatever quality assurance problem caused this glitch will be a thing of the past by the time of the next review.



## H+BEDV AntiVir/95 v1.00.3, 5.6.3

A couple of years ago, *H+BEDV's* virus detection engine performed remarkably well against the *VB* test-sets. It's not quite clear what has happened since then, but whatever it is, *AntiVir/95* needs a little work to catch up with the competition. An Overall In the Wild score of 83.8% leaves much to be desired, as does a Polymorphic rate of 67.0%.

Particularly weak is boot sector virus detection: a weakness in this area is fairly unusual. It proved impossible to persuade the on-access scanner to find any viruses in the boot sectors of diskettes used, which had a major effect on the on-access scan results.



Last virus found:
Hates.4000

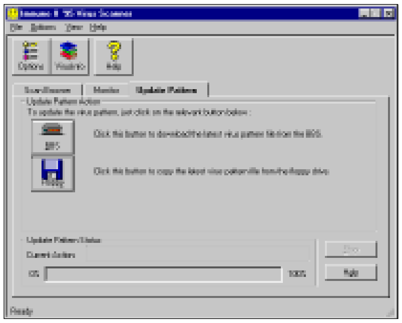
Number of files: 17
Time: 00:18

Viruses: 18
Repaired: 0
Deleted: 0

Folder: A:\
File: EMM386.EXE
Status: Searching

The interface is unremarkable, but easy to use, and it's worth having a look around for nice touches and puns – 'Luke Filewalker', anyone? The product also suffered an unfortunate nine false positives.

## Higher Ground IMMUNE II v2.0, VPN 244



Update Pattern Action

To update the virus pattern, just click on the relevant button below:

Click this button to download the latest virus pattern file from the BBS.

Click this button to copy the latest virus pattern file from the floppy drive.

Update Pattern Status

Current Action

Ready

*Higher Ground* is a company new to *VB* comparative reviews. Its product, *IMMUNE II*, appears very similar to that of *Trend* – indeed, it has '(c) Trend' messages all over it! The Virus Pattern Number (?) is well below that of the *Trend* product submitted for this review, so it is perhaps not surprising that it performs less impressively.

More surprisingly, it performs only fractionally worse than *Trend's PC-cillin* – a couple of percentage points in the Standard test-set is the only difference!

Aside from that, there does not seem to be very much to mention about *IMMUNE II* which is not discussed under the section on *Trend's* own product, *PC-cillin 97*.

## IBM AntiVirus v2.5.2c

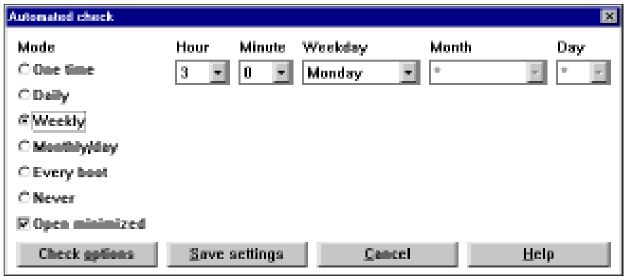
The second of the five 100% ItW Overall scores is obtained by *IBM* – impressive. The other on-demand results are almost as impressive: one sample (Argyle) missed in the Standard; a group of 500 (Mad.3544) in the Polymorphic.

Once again, *IBM's* technique of relying on checksums to speed the process of scanning data it has already seen comes up trumps: on the second scan of the clean hard drive, the product comes out far ahead of the rest, at over 6MB/second.

The version of the product which was submitted for review had a problem detecting viruses in files as they were opened. When executed, files were trapped by the on-access component without apparent difficulty, but when opened, they were more often than not missed. As discussed in the introduction, this part of the review had to be done on file access, not execution.

Consequently, the only figures obtained for the on-access scanner are in regard to its detection of boot sector viruses. It appears that the on-access bug has an impact on these figures as well: whereas the on-demand scanner found all 88 of the boot sector samples, the on-access one missed 27 of them. The problem is apparently fixed in the (you guessed it) upcoming version 3.0.

All that remains is to discuss the interface, which is unchanged from that seen a year ago. In most parts it is easy to use (it's very difficult to go wrong with one button labelled 'Press here' – a good thing), but is exceptionally spartan. For example, in one dialog that requires the user to enter the path to a file, there is no browse button, forcing the user to remember the path to the file and type it in, in full, by hand.



Mode
○ One time
○ Daily
● Weekly
○ Monthly/day
○ Every boot
○ Never
☑ Open minimized

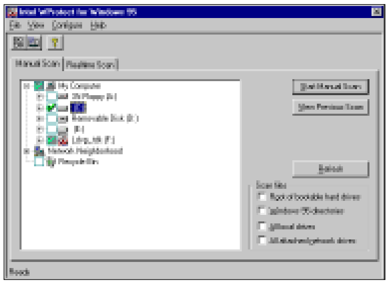
| Hour | Minute | Weekday | Month | Day |
|---|---|---|---|---|
| 3 | 0 | Monday | * | * |

| | Clean Floppy | | Infected Floppy | | Clean Hard Drive 1 | | Clean Hard Drive 2 | |
|---|---|---|---|---|---|---|---|---|
| | Scan Time (min:sec) | Data Rate (KB/s) | Scan Time (min:sec) | Data Rate (KB/s) | Scan Time (min:sec) | Data Rate (KB/s) | Scan Time (min:sec) | Data Rate (KB/s) |
| Alwil AVAST! | 0:39 | 25 | 1:12 | 16.3 | 12:40 | 702.8 | 12:40 | 702.8 |
| Cheyenne InocuLAN | 1:00 | 16.2 | 1:07 | 17.5 | 9:37 | 925.7 | 9:37 | 925.7 |
| Command F-PROT | 0:25 | 38.9 | 0:40 | 29.3 | 4:00 | 2225.5 | 4:00 | 2225.5 |
| Cybec VET | 0:27 | 36.1 | 0:36 | 32.6 | 2:45 | 3237.1 | 2:45 | 3237.1 |
| Dr Solomon's AVTK | 0:37 | 26.3 | 1:46 | 11.1 | 4:23 | 2030.8 | 4:23 | 2030.8 |
| EliaShim ViruSafe | 0:23 | 42.3 | 0:25 | 46.9 | 6:02 | 1475.5 | 6:02 | 1475.5 |
| ESaSS ThunderBYTE | 0:23 | 42.3 | 0:41 | 28.6 | 2:49 | 3160.4 | 2:49 | 3160.4 |
| H+BEDV AntiVir/95 | 0:32 | 30.4 | 0:37 | 31.7 | 5:35 | 1594.4 | 5:35 | 1594.4 |
| Higher Ground IMMUNE II | 0:32 | 30.4 | 0:48 | 24.4 | 6:10 | 1443.5 | 6:10 | 1443.5 |
| IBM AntiVirus | 0;32 | 30.4 | 0:36 | 32.6 | 10:23 | 857.3 | 1:26 | 6210.6 |
| Intel LANDesk Virus Protect | 0:33 | 29.5 | 0:54 | 21.7 | 6:13 | 1431.9 | 6:13 | 1431.9 |
| Iris AntiVirus Plus | 0:53 | 18.4 | 0:38 | 30.9 | 31:30 | 282.6 | 31:30 | 282.6 |
| KAMI AVP | 0:56 | 17.4 | 0:52 | 22.6 | 5:17 | 1684.9 | 5:17 | 1684.9 |
| McAfee Scan | 0:29 | 33.6 | 0:35 | 33.5 | 7:11 | 1239.2 | 7:11 | 1239.2 |
| Norman Virus Control | 0:48 | 20.3 | 1:07 | 17.5 | 9:15 | 962.4 | 9:15 | 962.4 |
| RG Software Vi-Spy | 0:26 | 37.4 | 0:36 | 32.6 | 3:34 | 2495.9 | 3:34 | 2495.9 |
| SafetyNet VirusNet | 0:30 | 32.5 | 0:42 | 27.9 | 4:38 | 1921.3 | 4:38 | 1921.3 |
| Sophos SWEEP | 0:36 | 27.0 | 0:31 | 37.8 | 5:13 | 1706.4 | 5:13 | 1706.4 |
| Stiller Research Integrity Master | 0:30 | 32.5 | 1:15 | 15.6 | 7:22 | 1208.4 | 7:22 | 1208.4 |
| Symantec Norton AntiVirus | 0:33 | 29.5 | 0:50 | 23.5 | 3:15 | 2605.4 | 3:15 | 2605.4 |
| Trend Micro PC-cillin 97 | 0:48 | 20.3 | 1:12 | 16.3 | 8:59 | 990.9 | 8:59 | 990.9 |

## Intel LANDesk Virus Protect v4.0 VPN 263

What is not clear is how *Intel*, which uses scanning technology from *Trend* (see box 'Who's using whom?') manages to provide a later signature file for review than *Trend* itself. Even more mysteriously, it resulted in lower scores than *Trend*! Oh well, just another of those mysteries…

*LANDesk Virus Protect* clocked up 96.4% in the In the Wild Overall with the on-demand scanner, and was on course to score the same with the on-access one when a problem was encountered. It was impossible to make it check boot sectors, so the product scored zero in this set. Scores in other areas are adequate, but could do with improvement.



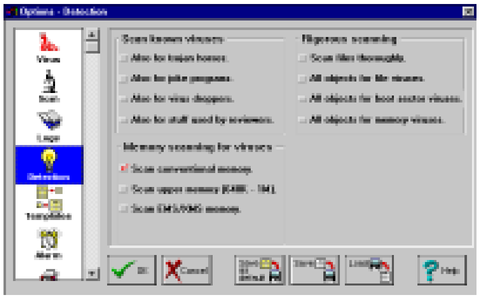
Scan files
☐ Root of bootable hard drives
☐ Windows 95 directories
☐ All local drives
☐ All attached network drives

The interface is very easy to use, and happily bears no resemblance to that last seen on the *Windows NT* version!

## Iris AntiVirus Plus v21.34

There was a time when *Virus Bulletin* was surprised when Iris scored well in comparative reviews. That time has gone now; we expect good things from this Israeli product. In this test, it does not disappoint: 99.6% in the Overall In the Wild section is an impressive result, as are the scores in the other sets. Its on-access component performs slightly less well than the on-demand one, but still satisfactorily.

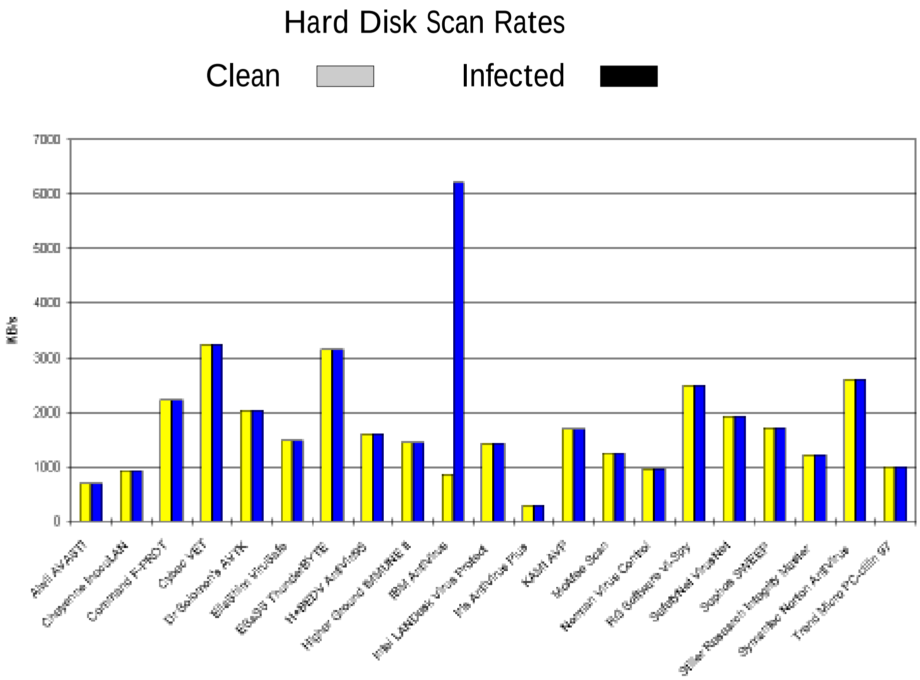
Alas, there were also downsides: there were two false positives, and the product was staggeringly slow on the test against the clean hard drive. The defaults provided by the scanner (which were, of course, used) seemed to have been



Scan known viruses
☐ Also for trojan horses.
☐ Also for joke programs.
☐ Also for virus droppers.
☐ Also for stuff used by reviewers.

Rigorous scanning
☐ Scan files thoroughly.
☐ All objects for file viruses.
☐ All objects for boot sector viruses.
☐ All objects for memory viruses.

Memory scanning for viruses
☑ Scan conventional memory.
☐ Scan upper memory (640K - 1M).
☐ Scan EMS/XMS memory.



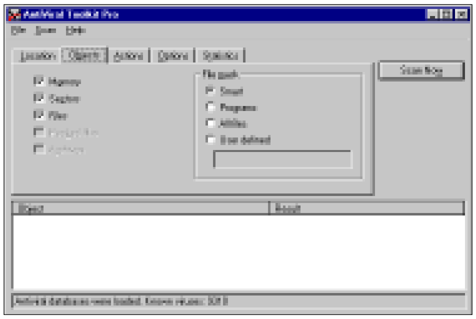
configured for the most enthusiastic scan permitted, which is unusual. Perhaps the installation routine misconfigured the scanner, resulting in such poor scan times?

The interface sports characteristic Borland buttons, and was slightly peculiar. It proved difficult (read 'impossible') to resize the parent window – this insisted on taking up the whole of the screen, and even then it appeared from the way some dialogs were drawn that it would have liked more room to spread itself.

Overall, Iris now has detection rates up amongst the top products. A little attention to speed, false positives, and interface detail will go a long way.

## Kami AVP v3.0b107

*Kami's* DOS scanner has long been known as the anti-virus equivalent of heavy artillery: when all else fails, wheel it out, point it in the vague direction of an infected computer, and it will sort out your problem. Well, now the developers of *AVP* have come up with versions of their product for other platforms, and the first of those to reach the pages of *Virus Bulletin* is that for *Windows 95*.



☑ Memory
☑ Sectors
☑ Files
☐ Packed files
☐ Archives

File mask
● Smart
○ Programs
○ All files
○ User defined

Antiviral databases were loaded. Known viruses: 3018

At this point, the product is clearly in the relatively early stages of its life: there is no on-access scanner, and some of the options dialogs are none too clear. In addition, detection rates are fractionally down since its earlier 'good old days'.

However, that doesn't stop this product from getting the third of the five 100% In the Wild Overall scores. It is in the other sets where the scores were slightly down – 93.4% in the Standard test-set, for example.

In addition to giving the product an interface, *AVP's* developers have been making the new product (another version 3!) faster – no longer at the bottom of the speed tests, it now resides comfortably around the middle of the field.

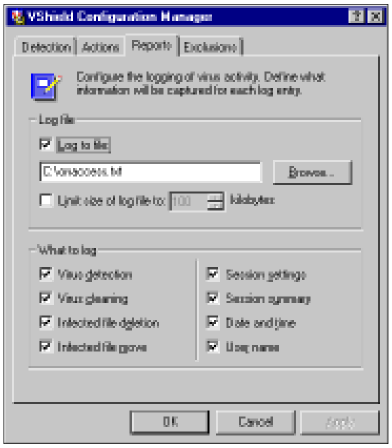
## McAfee Scan v3.0.0

It would appear that *McAfee* has been busy – the detection rates of the brand new (what else?) version 3 of their *Scan* have been significantly raised over those of previous versions. Exactly which parts of the product have been busiest is discussed in the box 'Who's using whom?', but for now suffice it to point out the sparkling 100% on-demand In the Wild Overall rate, and the equally spotless 100% on-demand Polymorphic score.

The on-access scanner has clearly not had the same modifications yet – its detection rates appear more like those we were expecting: high, but not perfect.

The product's interface remains a pleasure to use: uncannily similar to the *Windows 95* Find Files dialog, it is completely obvious which buttons need to be pushed to accomplish the various tasks.

Version 3 of *Scan* is slower than previous versions: it now sits in the middle of the scan speed field. Overall, this version offers significant improvements in the area of detection over previous versions, whilst having the benefit of remaining the same as far as the user interface is concerned.



Configure the logging of virus activity. Define what information will be captured for each log entry.

Log file

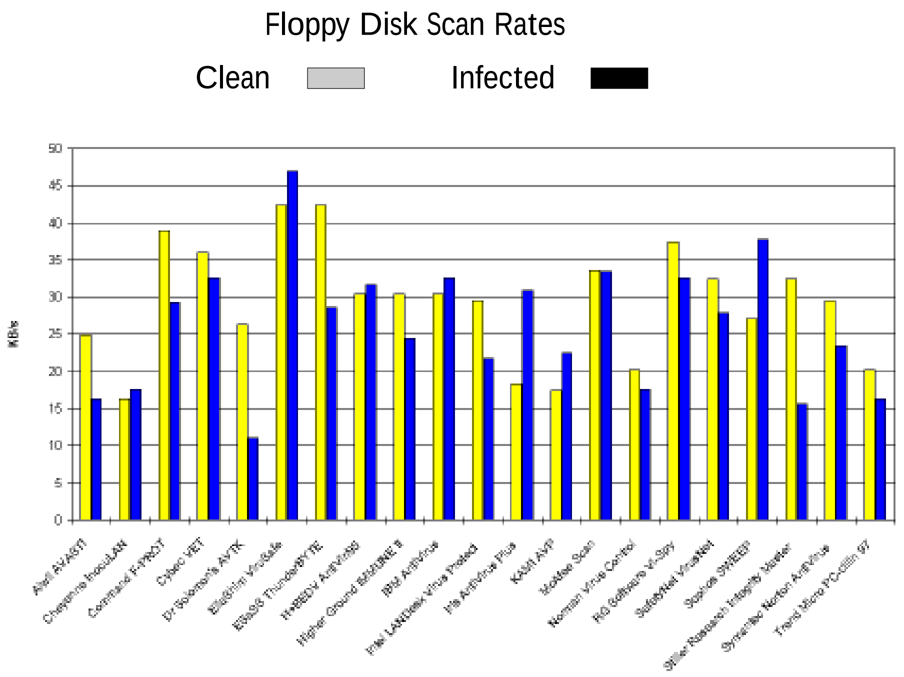
☑ Log to file

C:\vsaccess.txt

☐ Limit size of log file to: 100 kilobytes

What to log

☑ Virus detection
☑ Virus cleaning
☑ Infected file deletion
☑ Infected file move
☑ Session settings
☑ Session summary
☑ Date and time
☑ User name



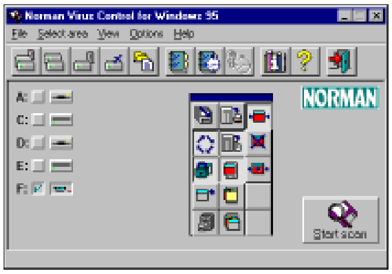
the *Windows* environment is that the user can utilize a *Windows* front-end to the essentially-command-line-driven scanner. The only problem with this approach is that it can look a little uninspiring to the user.

*Vi-Spy's* detection rates could do with a little improvement: 95% Overall on-demand ItW is under par. The on-access rates are virtually identical to those of the on-demand portion, but there was one occurrence of note here. Whilst the on-demand scanner can detect Hare.7750 in a boot sector, when the same diskette is presented to the on-access component, the system crashes.

In terms of speed, *Vi-Spy* comes out well above average, but it did encounter an unexpected nine false positives!

## Norman Virus Control v4.00, 28/02/97

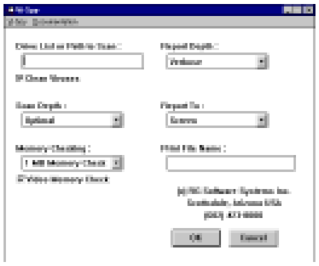
*NVC* misses out on 100% on-demand In the Wild detection by one virus; a sample of Satan_Bug. *Norman's* on-access component consists of a behaviour blocker, so it cannot be tested simply by copying files from one disk to another or opening and closing files – the files would need to be run. Consequently, no figures were obtained for its performance other than those gleaned against the Boot Sector test-set.



Considering the behaviour blocker claims to have no knowledge of specific viruses (in the traditional scanning sense), its score of 95.5% is impressive indeed.

The interface remains much as it was a year ago. Overall, it's a shame it couldn't achieve the 100% detection rate in all areas as its DOS companion did in the January comparative.

## RG Software Vi-Spy v15.0, 02/97



*RG's Vi-Spy* has also had no noticeable interface changes over the past year. It installs from a DOS session, then reverts to the *Windows 95* screen to install the program group and icons. After that, the sole visible concession to

## SafetyNet VirusNet v4.01

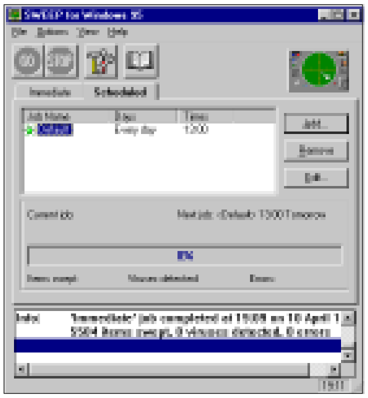
Another company new to *VB* comparatives, *SafetyNet's* product, *VirusNet*, is controlled from a colourful front-end depicting lightning over a city. This provides several buttons which access various parts of the product, including help, configuration, and the scanner.

The scanner's performance was somewhat disappointing: 88.3% on the In the Wild overall set could easily be bettered. Also, the on-access scanner could not be configured to check files on open, only on execute, so could not be adequately tested. Performance elsewhere was also unremarkable; particularly the 54.5% score on the Polymorphic set.

Considering the origins of this product's scanning technology (see panel 'Who's Using Whom?'), this poor performance is unexpected. *VB* looks forward to its next encounter with *VirusNet*.

## Sophos SWEEP v2.95

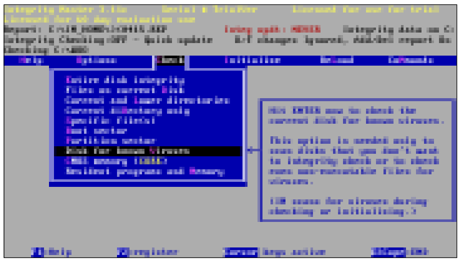
*Sophos' SWEEP* comes closest of all the products to a full house: two samples from the Standard test-set are all that stand between it and the perfect 100s. Its score is the same in the on-demand and on-access tests; however, its resident component (which is called InterCheck) does require the presence of a server on the network in order to function.



*SWEEP's* interface is pleasantly simple to use: the one serious complaint is that the keyboard shortcuts indicated on the menu bar (File, for example) do not work – the mouse must be used. In terms of speed, *SWEEP* is in the middle of the field. Overall, a good product.

## Stiller Research Integrity Master v3.11c

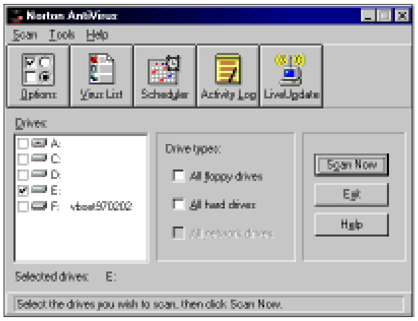
Once again, *Stiller Research* elected to submit its DOS scanner for a non-DOS review. There's nothing wrong with this, of course; it's just unlikely to fare that well in usability stakes. *Integrity Master's* interface is, well, unique (like that of *Cybec's VET*, but not) even in the DOS world. In amongst all these *Windows 95* products it appears decidedly different.



In this instance, unfortunately, in addition to having an interface that sticks out like a sore thumb, *Integrity Master* doesn't fare all that well in the detection stakes either. The score of 95% in the In the Wild Overall section appears high in numerical terms, but when compared to the other products in the test, it suddenly seems small. The 28.6% in the Polymorphic test-set, on the other hand, appears small to start with. All this is a shame, as the integrity-checking component is wonderful, and in spite of the idiosyncrasies of the interface, it's very usable.

## Symantec Norton AntiVirus, v2.0.1, 01/03/97

No major changes appear to have been inflicted on the user-visible pieces of this product, which is, in this case, a good thing. Detection rates are on the up, however: *Symantec's Norton AntiVirus* comes wading in with a frankly startling 99.8% in the In the Wild Overall column; it missed only one sample of Desperado.1403.C in these two test-sets. Polymorphic detection is a perfectly adequate 87.5% – not bad for this test. There were no false positives.



Drives: □ A: □ C: □ D: ☑ E: □ F: vbsat970202

Drive types: □ All floppy drives □ All hard drives □ All network drives

Selected drives: E:

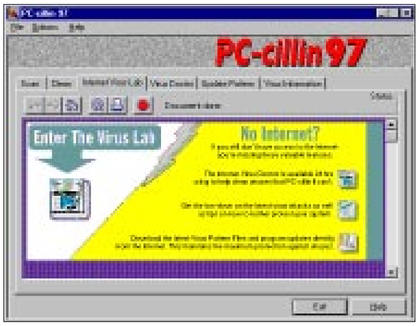
Select the drives you wish to scan, then click Scan Now.

Returning for a moment to the interface, *Symantec's* product offers something we will see more and more. The concept of updating your anti-virus product automatically has been around for a long time, but only comparatively recently has it become possible to arrange such things over the Internet. *NAV's* LiveUpdate feature handles this, although of course it is tricky to test such things from a network which is carefully isolated from everything else…

## Trend Micro PC-cillin 97 VPN 260

*PC-cillin* has gone through a couple of major revisions since last year. This fact caused some problems when it came to find a compatible serial number to install it. Once this was done, installation proceeded without difficulty.

It's not immediately obvious what has been done to the interface since last year, but whatever it is has made me like it a whole lot more. Its most notable new feature is the 'Virus Doctor': if you encounter suspicious or uncleanable files, you can submit them to the doctor for further analysis. Of course, what actually happens is that the file is emailed to *Trend*; the program appeared slightly confused as I tried to convince it that no, the test computer was not in fact connected to the Internet.



Anyway, detection rates are also improving, albeit not all that rapidly. *Trend* seems to be keeping pace with developments, as opposed to gaining any significant ground. Their interface wraps the product well, however, and offers other nice features such as automatic signature downloading.

### Comments

This review is notable not only for what is said, but for what is not. When compared with the same review approximately one year ago, the reader will notice that there are many fewer problems noted.

No mention has been made of installation programs: it was assumed (and indeed turned out to be the case) that there would be no problems in this area. The installation routine is the first part of the product a customer sees – if it doesn't work, he's liable to be understandably annoyed.

Also, less detail was used describing interfaces – the products appear to be, at least to some extent, converging on a single core appearance. As one example, many more now have tooltray icons to provide access to status displays and configuration options for the on-access components, so it is no longer worth commenting on such things. As time goes on, the standard which products for *Windows 95* are expected to reach goes up.

## Conclusions

One comment from the conclusions a year ago was the lack of general ‘*Windows 95*-ness’ – most products at that point did not really feel as if they belonged in the then-new environment. This is not the case any more: the majority of the products fit in much better than before.

### Who’s using whom?

One of the most interesting things about the anti-virus industry today is the difference between the number of products available and the number of engines available. Here, ‘engine’ means the component of the product that is left once you strip away interface and options; that part of the program which performs the task for which the product was purchased – finding viruses.

The virus world has got to such a point that it’s almost inconceivable that a new company could appear and suddenly start selling a new scanner. To the observer, scanners apparently appear out of nowhere, but this is simply because they have made it out of their country of origin and into the wider world. New anti-virus technology can appear, but it won’t be a scanner. Here is a list of anti-virus companies tested in recent *VB* comparatives, and their engines:

| | |
|---|---|
| Alwil | own |
| Cheyenne | Iris |
| Command Software | Frisk Software |
| Cybec | own |
| DataFellows | Frisk Software |
| Dr Solomon’s Software | own |
| EliaShim | own |
| ESaSS | own, but merging with that of Norman |
| Frisk Software | own |
| H+BEDV | own |
| Higher Ground | Trend |
| IBM | own |
| Iris | own |
| KAMI | own |
| Look! Software | Alwil |
| McAfee | own, but with components from Jade and Alwil |
| Norman | own, but merging with that of ESaSS |
| RG Software | own |
| SafetyNet | Alwil |
| Sophos | own |
| Stiller Research | own |
| Symantec | own |
| Trend | own |

Is there any problem with companies buying engines from others? Not really, but the buyer should be aware that perhaps some of the companies with the high detection rates don’t have the best anti-virus researchers after all…

Also encouraging is the number of products scoring well in the In the Wild sets: 19 of the 21 products achieved over 90% in this section; 11, over 99%; and five scored the maximum of 100% – a distinct improvement over a year ago. It is the In the Wild File and Boot sector test-sets that are the most important to the real-world user, and so it is here that the reader should concentrate most of his attention.

The other test-sets are not without their worth, however: the Polymorphic version is currently the hardest for products to perform well on (although *Virus Bulletin* intends to introduce a macro test-set in the near future, which may well prove the most difficult). In the polymorphic set, three products vie for the honours: *Dr Solomon’s*, *McAfee*, and *Sophos* all score 100%.

So, who wins? Well, regular readers will know that it’s never that simple. There can be no ‘Editor’s choice’ for anti-virus software; no five/four/three star awards; no ‘recommended’. It will always be horses for courses. However, in terms of detection, you’re not going to do any better than that offered by these three products: *Dr Solomon’s Software’s AVTK*, *McAfee Scan*, and *Sophos SWEEP*.

### TECHNICAL DETAILS

**Hardware used:** *Compaq ProLinea 590* (90MHz Pentium), 80MB RAM, 2.1GB hard disk, 270MB SyQuest drive, and external SCSI CD-ROM.

**Software:** *MS Windows 95* with Service Pack One installed.

**WildList used:** Both In theWild test-sets are based on theDecember 1996 WildList, available from http://www.virusbtn.com/WildLists/.

**Technical details:** With the exception of those making up the In the Wild Boot Sector test-set, virus samples are held on CD-ROM. Boot sector samples are stored on single 3.5-inch floppy diskettes.

**Calculation scheme:** See http://www.virusbtn.com/comparatives/win95/199705/protocol.html.

### TEST-SETS

**In the Wild Boot Sector viruses**

One sample each of the following 88 viruses: 15_Years, AntiCMOS.A, AntiCMOS.B, AntiEXE.A, Boot.437, BootEXE.451, Brasil, Bye, Chance.B, Chinese Fish, Crazy_Boot, Cruel, Da_Boys, Defo, DelCMOS.B, Den_Zuko.2.A, Diablo_Boot, Disk_Killer, Empire.Int_10.B, Empire.Monkey.A, Empire.Monkey.B, EXEBug.A, EXEBug.C, EXEBug.Hooker, FAT Avenger, Finnish_Sprayer, Flame, Form.A, Form.C, Form.D, Frankenstein, Galicia, Hare.7750, Ibex, Int40, J&M, Joshi.A, Jumper.A, Jumper.B, Junkie, Kampana.A, Leandro, Michelangelo.A, Moloch, Mongolian_Boot, Music_Bug, Natas.4744, Neuroquila, NYB, Ornate, Parity_Boot.A, Parity_Boot.B, Pasta, Peter, QRry, Quandary, Quiver, Quox.A, Ripper, Russian_Flag, Sampo, Satria.A, She_Has, Stealth_Boot.B, Stealth_Boot.C, Stoned.16.A, Stoned.Angelina.A, Stoned.Azusa.A, Stoned.Bunny.A, Stoned.Bravo, Stoned.Daniela, Stoned.Dinamo, Stoned.June_4th.A, Stoned.Kiev, Stoned.LZR, Stoned.Manitoba, Stoned.No_Int.A, Stoned.NOP, Stoned.Spirit, Stoned.Standard.A, Stoned.Swedish_Disaster, Stoned.W-Boot.A, Swiss_Boot, Unashamed, Urkel, V-Sign, WelcomB, and WXYC.

**In the Wild File viruses**

509 samples of the following 142 viruses (number of samples shown in brackets after virus name): Anticad.4096.Mozart (4), Alfons.1344 (5), Arianna.3375 (4), Avispa.D (2),

Backformat.2000.A (1), Bad_Sectors.3428 (5), Barrotes.1303 (6), Barrotes.1310.A (2), BootEXE.451 (3), Burglar.1150.A (3), Byway.A (1), Byway.B (1), Cascade.1701.A (3), Cascade.1704.A (3), Cawber (3), Changsa.A (5), Chaos.1241 (6), Chill (1), Cordobes.3334 (3), CPW.1527 (4), Dark_Avenger.1800.A (3), Delta.1163 (6), DelWin.1759 (3), Desperado.1403.C (2), Die_Hard (2), Digi.3547 (5), Dir_II.A (1), DR&ET.1710 (3), Ear.Leonard.1207 (3), Fairz (6), Fichv.2_1 (3), Flip.2153 (2), Flip.2343 (6), Freddy_Krueger (3), Frodo.Frodo.A (4), Ginger.2774 (2), Goldbug (3), Green_Caterpillar.1575.A (3), Hare.7610 (2), Hare.7750 (8), Hare.7786 (9), Helloween.1376.A (6), Hi.460 (3), Hidenowt (6), HLLC.Even_Beeper.B (3), Istanbul.1349 (6), June_12th.2660 (6), Jerusalem.1244 (6), Jerusalem.1500 (3), Jerusalem.1808.Standard (2), Jerusalem.Mummy.l364.A (3), Jerusalem.Sunday.A (2), Jerusalem.Zero_Time.Australian (3), Jos.1000 (3), Junkie (1), Kaos4 (6), Karnivali.1971 (3), Keypress.1232.A (2), Lemming.2160 (5), Liberty.2857.A (2), Little_Red.1465 (2), MacGyver.2803 (3), Major.1644 (3), Maltese_Amoeba (3), Mange_Tout.1099 (4), Manzon.1414 (2), Markt.1533 (3), Mirea.1788 (2), Natas.4744 (5), Necros.1164 (2), Nightfall.4518.B (2), No_Frills.Dudley (2), No_Frills.No_Frills.843 (2), Nomenklatura.A (6), Npox.963.A (2), November_17th.800.A (2), November_17th.855.A (2), One_Half.3544 (5), One_Half.3570 (3), Ontario.1024 (3), Pathogen:SMEG.0_1 (5), Ph33r.1332 (5), Phx.965 (3), Pieck.4444 (3), Plagiarist.2051 (3), Predator.2448 (2), Quicky.1376 (1), Reverse.948 (3), Sarampo.1371 (6), Sat_Bug.Sat_Bug (2), Sayha (5), Screaming_Fist.II.696 (6), Sibylle (3), Sleep_Walker.1266 (3), SVC.3103.A (2), Tanpro.524 (6), Tentacle.1996 (3), Tentacle.10634 (4), Tequila.A (3), Trojector.1463 (6), Trojector.1561 (3), Tai-Pan.438 (3), Tai-Pan.666 (2), Three_Tunes.1784 (6), Trakia.653 (3), Tremor.4000.A (6), TVPO.3873 (9), Unsnared.814 (3), Vacsina.TP-05.A (2), Vacsina.TP-16.A (1), Vampiro (2), Vienna.648.Reboot.A (3), Vinchuca (3), VLamix (3), Werewolf.1500.B (3), WM.Bandung.A (4), WM.Buero.A:De (4), WM.Colors.A (4), WM.Concept.A (4), WM.Concept.F (4), WM.Concept.J (4), WM.Date.A (4), WM.Divina.A (4), WM.Helper.A (4), WM.Hot.A (4), WM.Imposter.A (4), WM.Irish.A (4), WM.MDMA.A (4), WM.Nuclear.B (4), WM.Nop.A (4), WM.NPad.A (4), WM.Wazzu.A (4), WM.Wazzu.C (4), WM.Wazzu.E (4), WM.Wazzu.J (4), WM.Wazzu.P (4), Xeram.1664 (4), XL.Laroux (4), Xuxa.1984 (6), Yankee_Doodle.TP-39 (5), Yankee_Doodle.TP-44.A (5), and Yankee_Doodle.XPEH.4928 (2).

**Standard File viruses:**
765 samples of the following 319 viruses (the number of samples is shown in brackets after the virus name): Abbas.5660 (5), Accept.3773 (5), Account_Avenger.873 (3), Aforia.656 (6), AIDS (1), AIDS-II (1), Aiwed.852 (3), Alabama (1), Alexe.1287 (2), Algerian.1400 (3), Amazon.500 (2), Ambulance (1), Amoeba (2), Anarchy.6503 (5), Andreew.932 (3), Angels.1571 (3), Annihilator.673 (2), Another_World.707 (3), Anston.1960 (5), Anthrax (1), Anticad.4096.A (4), AntiGus.1570 (3), Anti-Pascal (5), Argyle (1), Armagedon.1079.A (1), Assignation.426 (3), Assassin.4834 (3), Attention.A (1), Auspar.990 (3), Autumnal.3072 (6), Baba.276 (3), Baba.356 (2), Backfont.905 (1), Barrotes.840 (3), Beast.498 (2), Bebe.1004 (1), Bell.390 (3), Big_Bang.346 (1), Bill.2658 (5), Billy.836 (3), BlackAdder.1015 (6), Black_Monday.1055 (2), Blood (1), Blue_Nine.925.A (3), Bosnia:TPE.1_4 (5), Burger (3), Burger.405.A (1), Burglar.824 (3), Butterfly.302.A (1), BW.Mayberry.499 (3), BW.Mayberry.604 (6), Cantando.857 (3), Cascade.1701.Jo-Jo.A (1), Cascade.1704.D (3), Casper (1), Catherine.1365 (3), CeCe.1998 (6), Cliff.1313 (3), CLI&HLT.1345 (6), CMOS.3622 (5), Coffeeshop (2), Cool.929 (3), Continua.502.B (3), Cosenza.3205 (2), Cowboy.2487 (2), Coyote.1103 (3), Cruncher (2), Crazy_Frog.1477 (3), Crazy_Lord.437 (2), Cybercide.2299 (3), Danish_Tiny.163.A (1), Danish_Tiny.333.A (1), Dark_Avenger.1449 (2), Dark_Avenger.2100.A (2), Dark_Revenge.1024 (3), Darkstar.439 (1), Datacrime_II (2), Datacrime (2), Datalock.920.A (3), DBF.1046 (2), Dei.1780 (4), Despair.633 (3), Destructor.A (1), Diamond.1024.B (1), Dir.691 (1), Discoloured_Star.223 (1), DOSHunter.483 (1), DotEater.A (1), Ear.405 (3), Eddie-2.651.A (3), Eight_Tunes.1971.A (1), Emhaka.749 (6), Enola_Gay.1883 (4), Entity.1980 (5), Fax_Free.1536.Topo.A (1), Fellowship (1), Feltan.565 (3), Finnish.357 (2), Fisher.1100 (1), Flash.688.A (1), Four_Seasons.1534 (3), Frodo.3584.A (2), Fumble.867.A (1), F-You.417.A (1), Genesis.226 (1), Glacier.1196 (2), Golden_Flowers.1688 (6), Gomer.691 (6), Gotcha.906 (6), Green.1036 (6), Greets.3000 (3), Greetings.297 (2), Halka.1000.b (3), Halloechen.2011.A (3), Hamme.1203 (6), Happy_New_Year.1600.A (1), Hasta.884 (2), HDZZ.566 (3), Helga.666.c (2), Helga.666 (2), Hideos.1028 (6), HLLC.Even_Beeper.A (1), HLLC.Halley (1), HLLP.5000 (5), HLLP.7000 (5), HN.1741 (3), Horsa.1185 (3), Hymn.1865.A (2), Hymn.1962.A (2), Hymn.2144 (2), Hypervisor.3128 (5), Ibqqz.562 (3), Icelandic.848.A (1), Immortal.2185 (2), Inferno.1800 (4), Internal.1381 (1), Intruder.2048 (3), Invisible.2926 (2), Itavir.3443 (1), IVP.1725 (3), Jerusalem.1607 (3), Jerusalem.1808.CT.A (4), Jerusalem.Fu_Manchu.B (2), Jerusalem.PcVrsDs (4), John.1962 (3), Joker (1), Joker.1570 (6), July_13th.1201 (1), June8th.1919 (6), June_16th.879 (1), Kamikaze (1), Kela.b.2018 (3), Kemerovo.257.A (1), Keypress.1280 (6), Khizhnjak.556 (3), Kode.145 (3), Korea_Eddy.1316 (6), Korea_Miny.218 (3), Korea_Wanderer.1756 (6), Kranz.255 (3), Kukac.488 (1), Lauren.632 (3), Lavi.1460 (3), Leapfrog.A (1), Leda.820 (3), Lehigh.555.A (1), Liata.327 (3), Liberty.2857.A (5), Liberty.2857.D (2), Liquid_Power.1016 (3), Little_Brother.307 (1), Loren.1387 (2), Lost_Love.853 (6), LoveChild.488 (1), Lutil.591 (3), Maresme.1062 (3), MemLapse.289 (3), Metabolis.1173 (3), Mickie.1100 (3), Midin.765 (2), MonAmi.1085 (3), Monster.424 (3), Mothership.655 (3), MPC.442.c (3), Mummy.1353 (3), Necropolis.1963.A (1), Nina.A (1), November_17th.768.A (2), NRLG.1038 (3), NutCracker.3500.D (5), Odious.569 (3), Omud.512 (1), On_64 (1), Oropax.A (1), Pamyat.2000 (2), Parity.A (1), Paulus.1804 (5), Peanut (1), Perfume.765.A (1), Phantom1 (2), Phoenix.800 (1), Pitch.593 (1), Piter.A (2), Pixel.847.Hello (2), Pizelun (4), Plague.2647 (2), Poison.2436 (1), Pojer.4028 (2), Positron (2), Power_Pump.1 (1), Prudents.1205.A (1), PS-MPC.227 (3), PS-MPC.545 (6), QPA.256 (3), Quark.A (1), Red_Diavolyata.830.A (1), Revenge.1127 (1), Riihi.132 (1), Rmc.1551 (4), Rogue.1208 (6), Rosebud.912 (3), Rubbit.734 (2), Saturday_14th.669.A (1), Screaming_Fist.927 (4), Screen+1.948.A (1), SillyCR.710 (3), Selfex.1472 (6), Semtex.1000.B (1), Senorita.885 (3), Shake.476.A (1), ShineAway.620 (3), SI.A (1), SillyC.226 (3), SillyCR.303 (3), Sofia.432 (3), Soup.1073 (3), Spanz.639 (2), Stardot.789.A (6), Stardot.789.D (2), Steatoda (6), Stud.347 (3), Subliminal (1), Suomi.1008.A (1), Suriv_1.April_1st.A (1), Suriv_2.B (1), Surprise.1318 (1), SVC.1689.A (2), Svir.512 (1), Svin.252 (3), SysLock.3551.H (2), Sylvia.1332.A (1), TenBytes.1451.A (1), Teraz.2717 (5), Terror.1085 (1), Thanksgiving.1253 (1), The_Rat (1), Tigre.1795 (6), Tiny.133 (1), Tiny.134 (1), Tiny.138 (1), Tiny.143 (1), Tiny.154 (1), Tiny.156 (1), Tiny.158 (1), Tiny.159 (1), Tiny.160 (1), Tiny.167 (1), Tiny.198 (1), Todor.1993 (2), Traceback.3066.A (2), Trivial.113 (3), TUQ.453 (1), Untimely.666 (3), V2P6 (1), V2Px.1260 (1), Vacsina.1212 (1), Vacsina.1269 (1), Vacsina.1753 (1), Vacsina.1760 (1), Vacsina.1805 (1), Vacsina.2568 (1), Vacsina.634 (1), Vacsina.700 (2), Vbasic.5120.A (1), VCC.350 (3), Vcomm.637.A (2), VCS1077.M (1), VFSI (1), Victor (1), Vienna.583.A (1), Vienna.623.A (1), Vienna.648.Lisbon.A (1), Vienna.Bua (3), Vienna.Monxla.A (1), Vienna.W-13.507.B (1), Vienna.W-13.534.A (1), Vienna.W-13.600 (3), Virogen.Pinworm (6), Virus-101 (1), Virus-90 (1), Voronezh.600.A (1), Voronezh.1600.A (2), VP (1), Warchild.886 (3), Warrior.1024 (1), Whale (1), Willow.1870 (1), WinVir (1), WW.217.A (1), XWG.1333 (3), Yankee_Doodle.1049 (1), Yankee_Doodle.2756 (1), Yankee_Doodle.2901 (1), Yankee_Doodle.2932 (1), Yankee_Doodle.2981 (1), Yankee_Doodle.2997 (1), Zany.225 (3), Zero_Bug.1536.A (1), and Zherkov.1023.A (1).

**Polymorphic File viruses**
12,000 samples of each of the following twenty-four viruses (500 of each): Alive.4000, Anarchy.6503, Arianna.3076, Code.3952:VICE.05, Cordobes.3334, Digi.3547, DSCE.Demo, Girafe:TPE, Gripe.1985, Groove and Coffeeshop, Mad.3544, MTZ.4510, Natas.4744, Neuroquila.A, Nightfall.4559.B, One_Half.3544, Pathogen:SMEG.0_1, PeaceKeeper.B, Russel.3072.A, SatanBug.5000.A, Sepultura:MtE-Small, SMEG_v0.3, Tequila.A, and Uruguay.4.

# PRODUCT REVIEW 1

## ToothBrush

Dr Keith Jackson

*ToothBrush* calls itself a ‘Disk Authorisation, Access Control and Anti-Virus Management’ program. The word ‘management’ refers to the product’s ability to enforce any anti-virus program; either *ToothBrush’s* own program, which only lets data files arrive on a floppy disk, or any other scanner.

The *ToothBrush* manual (a disk file) insists ‘You may think this is quite a complicated specification’. I disagree: it sounds simpler than some of the disk-hoggers I have reviewed for *VB*. *ToothBrush* can operate from a network, and can be installed/upgraded by downloading from a network.

### Documentation

The documentation provided with the review copy was contained on disk, in a file called MANUAL.TXT. This was an unstructured text file which provided a reasonable explanation of how to install and use *ToothBrush*, but would be no help whatever if trouble arose: there is no consideration of what types of error may occur, no documentation of the possible error messages, no glossary, and no index.

Nowadays, many products provide on-line documentation: when done properly, this works very well. In some cases I have seen, it is even better than traditional paper-based documentation. It must be said, however, that I remain basically unimpressed by the help available in this product. It needs more work, and should expend more time dealing with problems rather than explaining what is blindingly obvious from a cursory (geddit?) glance at the screen.

### Installation

*ToothBrush* was provided for review on a single 1.44MB, 3.5-inch floppy disk containing 21 files in 621KB of disk space. The floppy disk arrived in a CD-style case.

Unlike last month’s product, *ToothBrush* explicitly reminds users that they should copy the distribution disks before *ToothBrush* is installed. None of this ‘writing back to an original master’ malarkey.

Installation of *ToothBrush* proved straightforward. A subdirectory to contain its files has to be nominated, then the PC must be defined as a ‘Gateway’ (or not). The *ToothBrush* manual defines a Gateway as ‘a PC that contains various virus scanning products and uses these to authorise a floppy disk for use on other PCs within your company’.

The presence of various *ToothBrush* utilities (CLEANBOO, DATAONLY, see below) must next be confirmed; then the configuration program searches the hard disk for anti-virus programs – it found *Dr Solomon’s Anti-Virus Toolkit* and *Sophos SWEEP*. These were added to the list of programs used to carry out validation checks on floppy disks.

Although *ToothBrush* is being very practical in looking for anti-virus programs, it adds DATAONLY, its own data analyser (which merely checks that no executable files are present on a floppy disk) to this list, then states that ‘All scanners will be ignored in favour of Data Analyser’. I would expect the default to be that *all* checks are performed, not just those provided by default.

When installation was complete, *ToothBrush* had installed Bootup Protection, Ctrl+Break Inhibit, File Protection and Disk Authorisation features. It had installed just nine files, occupying only 213KB, in its own subdirectory – this was despite the fact that I accepted every option that was offered during installation. Impressive.

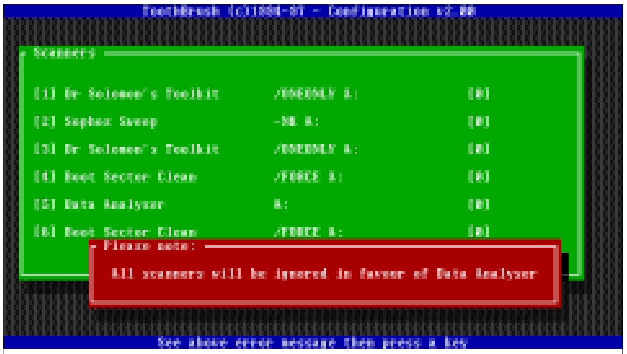
After the installation process, a reboot is necessary before *ToothBrush’s* features become active. Although the product added a memory-resident program to the file CONFIG.SYS (see below), AUTOEXEC.BAT remained unaltered.

The disk-locking facility provided with *ToothBrush* has not been reviewed, as text inside the program INSTALL.EXE stated that ‘The disk locking facility is disabled in this evaluation copy’.

### Configuration

*ToothBrush* is configured using a DOS program called ECONFIG. Permission to format and/or write to floppies can be switched on/off at will. Likewise, diskette-formatting can be enabled or disabled. If a floppy disk is formatted on a PC protected by *ToothBrush*, it is automatically authorized.

When a *Toothbrush*-protected PC is used, memory-resident software examines all floppy disks to ensure that each carries a valid ‘authorization code’. This can either be a simple signature, or can comprise a signature plus a CRC.



```
ToothBrush (c)1990-97 - Configuration v2.00

Scanners

[1] Dr Solomon's Toolkit      /ONEONLY A:          [0]
[2] Sophos Sweep              -NK A:               [0]
[3] Dr Solomon's Toolkit      /ONEONLY A:          [0]
[4] Boot Sector Clean         /FORCE A:            [0]
[5] Data Analyser             A:                   [0]
[6] Boot Sector Clean         /FORCE A:            [0]

Please note:
All scanners will be ignored in favour of Data Analyser

See above error message then press a key
```

The configuration program was easily able to detect the presence of *Dr Solomon’s AVTK* and *Sophos SWEEP*.

ECONFIG allows either mode of operation to be selected, but a decision on which to use should be taken with care, as switching between the two modes requires all floppy disks to be reauthorized – a slow and tedious process.

### Memory-resident Software

ToothBrush installs a memory-resident device driver which contains the software to enforce floppy disk authorization requirements. The manual states that this device driver is 'quite compact' – at 10.7KB, I must agree.

On a one-off basis, the *ToothBrush* device driver can be prevented from entering memory by holding down a special key combination whilst the PC boots, and confirming this request by entry of a correct password. The device driver is automatically reloaded when the PC is next rebooted.

*ToothBrush* prevents any unwanted attempts to change file attributes. A general ban on writing to disk can be enforced by *ToothBrush*, or a more selective policy can be invoked. CONFIG.SYS is always protected from alteration (this prevents *ToothBrush* being disabled).

Whenever *ToothBrush's* memory-resident software detects an unauthorized floppy, it does prevent access. Blocking access like this inevitably results in some apparently strange errors being reported; initially, it seemed odd to receive a 'write-protected' error message on a non-write-protected floppy.

### Bootup Protection

When *ToothBrush's* boot protection has been installed, the PC will enforce entry of a password before it will complete a boot. I cannot find much either to review or criticize about this process – it works; *ToothBrush* does indeed prevent rebooting unless a correct password is entered.

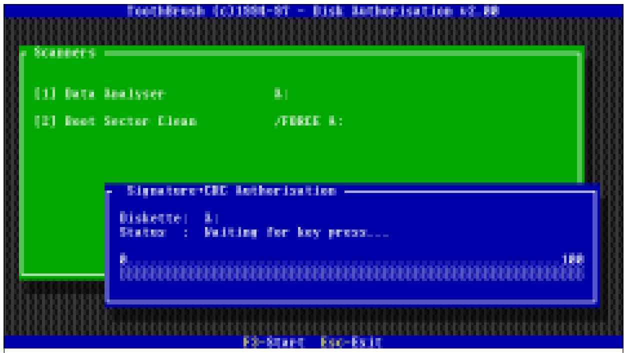
A utility called CLEANBOO is provided with *ToothBrush* which overwrites the existing floppy disk boot sector with its own code. On my test PC, CLEANBOO took three seconds to write a new boot sector to a floppy disk.

The manual claims that CLEANBOO will automatically remove 'ANY boot sector virus that may be on the disk EVEN if that virus is new and unknown to any of the virus scanners'. This sounds grandiose, but many products on the market include the same feature. Note that *ToothBrush* does not claim to stop all viruses, just boot sector viruses, which can usually be eradicated merely by over-writing them.

If a reboot from an authorized diskette is accidentally made, an onscreen warning message states 'Remove floppy from drive & REBOOT', and the PC buzzer sounds continuously. This is probably the product's single most useful feature.

### Floppy Disk Authorization

Authorization is performed using EAUTHOR – execution of this program is password-protected (this is optional). The program adds an authorization code to a floppy disk which is determined by the registration details supplied when *ToothBrush* was first installed (also by date/time of installation). This makes the authorization codes for each individual *ToothBrush* installation unique. Registration is thus very important – not the usual device to ensure that marketing people can send you endless piles of unwanted rubbish.



```
ToothBrush (c)1990-97 - Disk Authorisation v2.00
Scanners
[1] Data Analyser            A:
[2] Boot Sector Clean        /FORCE A:
Signature+CRC Authorisation
Diskette:  A:
Status  :  Waiting for key press...
0                                          100
F3-Start  Esc-Exit
```

Signature+CRC authorization prevents floppies being altered on PCs not protected by *ToothBrush*.

Authorization is performed by inserting the floppy disks in the PC and pressing a key. The process is almost trivial, and once again I am at a loss as to how to review this process. It works. What more is there to say?

The authorization program executes a series of programs which check the disk contents. These could be any scanner program (*ToothBrush* searches the hard disk and looks for the scanners of which it has knowledge), *ToothBrush's* own DATAONLY (which just permits use of floppies which contain only data), and/or software that will force a 'clean' boot sector on to the floppy. If all checks are passed, then (and only then) will *ToothBrush* authorize the floppy disk.

When files are added to or deleted from the floppy disk on a PC which is using the valid *ToothBrush* device driver, the checksum will change in sympathy. If changes are made to the content of the floppy on a PC which does not use *ToothBrush*, the floppy disk must be reauthorized before *ToothBrush* will accept it.

If EAUTHOR is left unused for one minute, password entry is enforced before it will restart. After two minutes of inactivity, a 'bouncing ball' screen saver activates.

### Authorization Oddities

When a floppy disk authorized by *ToothBrush* was inspected using *Norton Commander* (a well-known, long-standing DOS user interface), strange things ensued. *Norton Commander* thought that the root subdirectory of the floppy disk comprised 180 subdirectories, each with the name '........:...', and each subdirectory was dated 22/07/03 and timed at 30:55 (I'm not making this up!). Trying to access any of these subdirectories produced the error message 'Error on drive A:, disk may not be formatted'.

I am not sure what *ToothBrush* has done to the floppy disk ; the information which was provided does not permit me to judge this. However, if any *Norton Commander* users are out there, they should beware. It may be the case that other user interface programs will have similar problems with this product.

Do not try taking DATAONLY out of *ToothBrush's* list of programs that can be used to validate disks before authorization proceeds. If you do, and subsequently try to reinsert DATAONLY, *ToothBrush* will fail to find it. *ToothBrush* assumes that DATAONLY is contained in a subdirectory called C:\ENFORCER, despite the fact that, at installation time, I accepted the *ToothBrush* default subdirectory of C:\TBRUSH. Somebody forgot to amend the ENFORCER code when it was introduced to *ToothBrush* perhaps?

### Overhead

The 'signature only' mode of operation means diskette access will only be permitted if the floppy contains the correct authorization code. This does not prevent floppies being altered on PCs not protected by a compatible version of *ToothBrush*.

Signature+CRC operation means the floppy disk will also be checksummed to ensure the contents match the current value of the checksum – this prevents floppies which have been altered from being used on non-*ToothBrush* protected PCs. This mode is slower than signature alone, but more secure.

Authorization of an empty floppy disk took 17.5 seconds on my test PC. When half full (17 files, 703KB), the floppy was authorized with signature alone – with DATAONLY active, the time rose to 58 seconds. When signature+CRC was used, authorization time rose again to 61 seconds.

The execution of DATAONLY in these last tests occupied 52 seconds; by far the longest part of the whole process. If other scanners are used, the time taken for authorization may vary enormously.

Formatting a floppy disk is also affected by the presence of *ToothBrush*, though the formatting process itself takes so long that the overhead of authorization is minimal. For instance, using the figures from the previous paragraph and subtracting the effect of DATAONLY, authorization adds just six seconds to the time required to format a floppy disk. Given that the disk-formatting process took several minutes (dependent on the type of format invoked), the authorization overhead is placed in its true context – negligible.

Even merely looking at a directory listing involves a slight *ToothBrush* overhead. On my test PC, a directory listing of a floppy disk subdirectory normally produced in 4.1 seconds took 4.6 seconds when signature only authorization was in use, and 4.9 seconds when signature+CRC authorization was in use. Small, but measurable.

### Stopping Executable Code

DATAONLY will only execute as part of EAUTHOR; it refuses to execute as a stand-alone program. I know not why. It would be more useful if it did.

When DATAONLY executes, it inspects every file on the disk, searching for anything executable. DATAONLY always found EXE files (whatever their extension), but missed renamed COM files – perhaps this is unsurprising. In addition, DATAONLY can look inside ARJ archives for executable files.

As stated, when 'executable' files are renamed, DATAONLY can still spot EXE files, but misses COM files. It also misses BAT files, and renamed ARJ files – curious, as these latter have a distinctive header. DATAONLY must be using the file header to identify EXEs, so why not ARJs as well?

### Windows

When *Windows* is first executed after *ToothBrush* has been installed, the only obvious difference is an extra *ToothBrush* icon, available immediately after reboot. The code associated with this icon is used to communicate *ToothBrush* error messages in *Windows* form.

That's about it for *Windows*: the product works as normal; access is permitted only to authorized floppy disks. All its utilities are available under *Windows* (e.g. EAUTHOR can be used to authorize floppy disk), but remember they are all DOS programs. Nothing is *Windows*-specific.

### Conclusions

*ToothBrush* provides anti-virus features that should help prevent viruses gaining access to a PC. It doesn't really do very much, but what is claimed to work, does.

However, as described above, a few problems remain. I will not list the problems again – suffice it to say that on the whole they remain fairly minor.

This product is a collaborative venture between developer *Precise Publishing* and vendor *Ethan Adams*. The latter states that the latest version is more robust, and that work is in hand on a more comprehensive paper-based support manual.

**Technical Details**

**Product:** *ToothBrush v2.18a* (no serial number visible).

**Developer:** *Precise Publishing Ltd*, The Old Vicarage, Colley Gate, Halesowen, West Midlands B63 2BU, England. Tel +44 1384 560527.

**Vendor:** *Ethan Adams & Associates Ltd*, 70 Tamworth Road, Ashby de la Zouche, Leicestershire LE65 2PR, England. Tel +44 1530 565900, fax +44 1530 560570, email sales@ethan-adams.co.uk, http://www.ethan-adams.co.uk/.

**Availability:** A PC operating under DOS, *Windows 3.1*, or *Windows 95* operating systems.

**Price:** Single-user licence £29.95; multiples on application.

**Hardware used:** Toshiba 3100SX, a 16MHz 386 laptop, with 5MB of RAM, a 3.5-inch (1.44MB) floppy disk drive, and a 40MB hard disk, running under *MS-DOS v5.0* and *Windows v3.1*. Regular readers of my reviews should say goodbye to this much-loved machine, as *VB* has deemed it to be much too old, an antique even, and has provided a shiny new *Pentium* on which future reviews will be performed. Goodbye old friend after nearly eight years of faithful service. Sob.

# PRODUCT REVIEW 2

## NetShield for Windows NT

*Martyn Perry*

This month's review looks at *McAfee's* anti-virus scanner for *Windows NT*. The product was supplied on CD-ROM, along with a hard copy of the user's guide. The licence (included in the guide) lasts for two years, and covers the server and a defined maximum number of PCs. It also includes phone support and on-line product updates from the *McAfee* BBS or WWW site. For an additional annual charge, customers can have updates shipped quarterly on CD.

### Presentation and Installation

The documentation is clear and concise. In addition to the user manual, a White Paper provides a 'management report' on the status of the virus arena. Though this acts as lead-in to a justification for selecting *McAfee* products [*of course! Ed.*], it nevertheless provides useful facts and statistics to present to management. An additional pamphlet describes how to access the *McAfee* BBS from various operating systems.

Installation involves running SETUP.EXE. The first choices determine the type of installation: Compact, Typical, or Custom. A Compact installation installs only server components. Under Typical, the default set (Console, Server, and Alert Manager) is automatically installed. Finally, a Custom installation allows selection of which components to install.

These options provide the flexibility to set up servers to local requirements. Further options are: start the Task Manager at boot time, start Task Manager at the end of the setup process, and add a shell extension to support a new entry in the context-sensitive *Explorer* menus.

At this point a user name with Administrator rights, and that account's password, may be given; otherwise, the system account is used. In the Typical installation, *McAfee's* Alert Manager and Task Manager are added to the Services List. If the option to restart the PC is chosen, the *NetShield* icon is loaded into the Tool Tray (next to the clock on the Start bar).

In recognition of the fact that *McAfee* products have been attacked in the past, and as a way of checking for file corruption, there is a validation (checksum) facility. This allows the size of the various files to be checked against the shipping manifest, and offers limited protection for the user (all that needs to be done to defeat this is to change the manifest at the same time as sabotaging the programs themselves).

### Operation

The operation of *NetShield NT* is based around the concept of 'Tasks'. These Tasks consist of the various scan and action options which are available when scanning for viruses. The Tasks split into two main groups: On-access and On-demand. The latter group can be further subdivided, into Immediate and Scheduled Tasks.

On-access Tasks can monitor files copied to and from the server, depending on how it is configured. The files can be program files with defined extensions, or all files. Should a virus be detected, certain actions are available to the user: deny access to infected files and continue, move infected files to a folder, clean infected files automatically, or delete infected files automatically.

In addition, there are two network connection options; one to alert the client and the other to disconnect the offending workstation. There are two default exclusions from the scan: PAGEFILE.SYS and McAfee\NetShield NT directory.

The main way to initiate an Immediate Scan is through the GUI via the Start menu (*NT 4.0*) and/or the Program Manager (*NT 3.51*). It can also be accessed via the command-line (the command-line executable is called SCAN32.EXE). Scan progress is displayed using a series of animations.

The immediate scanner can be stopped part-way through a scan and subsequently restarted if required. In the latest version, the default executable file extensions for all types of scan have been rationalized to COM, EXE, DO*, and XL*. A choice is available between scanning the whole drive on a PC, or a specific path and its associated subdirectories. Specific files can also be scanned.

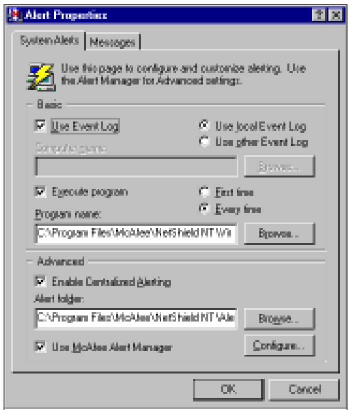
A Scheduled Scan can be configured to run once, or periodically – hourly, daily (with a choice of which days), weekly, monthly, or every time the server is started. The scanner does not handle overlapping schedules, so only one scheduled task can be in progress at any one time. *McAfee* states that in version 3.0 this problem has been resolved.

### Administration

If the user is logged in as Administrator (or as administrator-equivalent), no additional password is required to access the scanner administration. The administration program creates and manages the various tasks, and the main menu gives access to the various configuration options.

The scan menu provides the ability to create, delete, start, and enable/disable a task. Although setting up a task is straightforward, a Scan Wizard is also offered, allowing a user to step through the process of setting up a task. This may provide useful support to a new user, but more experienced users will probably not require it.

The edit menu allows tasks to be copied and pasted, and the importing and exporting of specific tasks. The ability to cut and paste tasks allows multiple tasks to be set up quickly



Use this page to configure and customize alerting. Use the Alert Manager for Advanced settings.

Basic

☑ Use Event Log
● Use local Event Log
○ Use other Event Log

Computer name:

☑ Execute program
○ First time
● Every time

Program name: C:\Program Files\McAfee\NetShield NT\Wi

Advanced

☑ Enable Centralized Alerting

Alert folder: C:\Program Files\McAfee\NetShield NT\Ale

☑ Use McAfee Alert Manager

There are various methods of customizing alert settings.

and consistently. The Import and Export options are concerned with moving the configuration files (that is, VSC files) from one computer to another. These configuration files hold all of the pre-defined settings for any particular scanning tasks.

CONFIG.VSC, the default configuration file, holds a number of settings for the SCAN32 programs. The file is formatted in a manner similar to most *Windows* INI files. The settings are arranged into five groups: ScanOptions, AlertOptions, ActivityLogOptions, Scheduler and TaskDefinitions. A separate command-line utility, called IMPTASK, allows tasks to be broadcast to multiple computers. This could be used as part of a batch file for automatic configuration of remote computers.

The view menu selects whether the toolbar and status bars are displayed, and the tools menu gives access to the list of viruses. The ability to connect to other PCs is available, as is the option to monitor the contents of the event log. There are also options for auto-updating virus signatures, and for configuring the alert management.

## On-demand Scanning

The on-demand scanner (SCAN32) can operate in a number of modes, from the command-line or a GUI:

- SCAN32 [switches] [scan items] – uses the various command-line switches to scan specific items
- SCAN32 <CONFIG.VSC> [override switches] [override scan items] – here, the scanner uses the settings defined in the configuration file but can also override the selections with temporary selections
- SCAN32 [/SERVER <servername>] /TASK <taskid> [override switches] [override scan items] – in this mode, the scanner uses tasks defined by the Console program and the settings stored in the registry key HLM\SOFTWARE\McAfee\NetShield\Tasks (HLM stands for HKEY_LOCAL_MACHINE). If a server name is included, the task information is taken from that server's registry, otherwise it comes from the local registry. Again, a temporary override is available.

## Reports and Activity Logs

As well as the responses available when a virus is detected (cleaning, moving deleting etc), *NetShield NT* can log virus incidents in an Event Log. This log may be on the local machine or on a remote computer.

In addition, it can run a program either the first time a virus is detected, or every time one is found. This can be used if the Alert Manager does not meet the user's needs; e.g. to communicate with an unsupported email system. To augment the options, *NetShield NT* incorporates an Alert Manager, which provides the ability to inform specified users of an event via different communications media; mamely a printer, another computer running *NetShield*, a network message to defined computers, Pagers, and SMTP email.

All of these can be defined to receive low, medium, or high priority alerts. Further, *NetShield NT* supports SNMP. The alert messages can be configured to include the name of the infected file, the name of the virus, the *NetShield* task which detected the virus, and the date and time of the event. Priorities for alerting may be customized by the administrator.

To assist with setting up these alerts, a text-string can be created to simulate a test virus for checking the correct operation of alerts. This is the EICAR Standard AntiVirus Test File, and is supplied in text form in the Help file on the CD-ROM. This can be cut and pasted into a 69-byte text file which can be renamed EICAR.COM.

## Updates

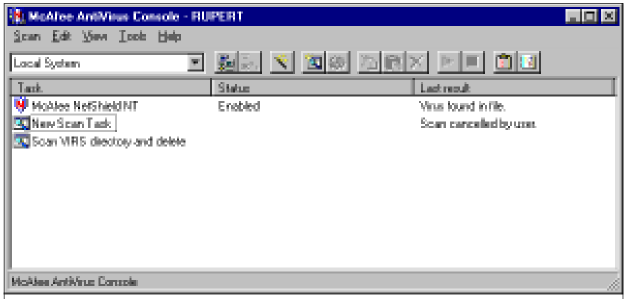
Approximately once a month, *McAfee* produces updates to the virus signatures, etc. These are available on the company BBS, from its Internet site, and via CompuServe.

*NetShield NT* provides an Auto-update program which gives the option to download the new version automatically. This updated version can be obtained either from a distribution site, e.g. a server on the network, or from the Internet by using a script for automating the FTP transfer. Once the transfer is complete, the information can be made available for access by other computers.

The Auto-update program can thus be configured so one main server dials up for updates from the *McAfee* site and deposits them into a target area. This can then be defined as the source of updates for all other servers on the network.

## Detection Rates

The scanner was checked using the usual three test-sets; In the Wild, Standard and Polymorphic (see summary for details). The tests were conducted using the default scanner



| Task | Status | Last result |
|---|---|---|
| McAfee NetShield NT | Enabled | Virus found in file. |
| New Scan Task | | Scan cancelled by user. |
| Scan VIRS directory and delete | | |

The scanner console gives the status of the various tasks.

file extensions supplied. The scan action option was selected to move the infected files, and the residual file count used to determine the detection rate. The virus signatures used were from *NetShield 2.5.3a* and were dated 4 February 1997.

The In the Wild result missed a perfect score by only two samples. The Standard test missed 44, giving only 91.7%. The product struggled with some of the polymorphics, missing 1803 samples. All 500 samples of Anarchy, DSCE.Demo and PeaceKeeper.B were missed completely, as were just over a quarter of those of Sepeltura:MTE-Small. The remaining misses were Girafe:TPE and Gripe.1985.

### Real-time Scanning Overhead

To determine the impact of the scanner on the workstation when it is running, we timed how long it took to copy 200 files (20.55 MB, EXE and COM files) from one directory to another using XCOPY. The directories used for source and target were excluded to prevent a file being scanned while waiting to be copied. The default setting (Maximum Boost for Foreground Application) was used. Due to the different processes which occur within the server, the tests were run ten times for each setting and an average taken. The tests were:

- Program not loaded: establishes the baseline time for copying the files on the server
- Program unloaded: run after the other tests to check how well the server returns to its former state
- Program loaded without Incoming or Outgoing on-access tests running: tests the impact of the application in a quiescent state
- Program loaded with just Incoming on-access checks running: tests the impact of the real-time scan for just reading the files.
- Program loaded; both Incoming and Outgoing on-access checks running: shows full overhead of real-time scans
- Program loaded; Incoming and Outgoing on-access checks; Immediate scan running: full impact of running real-time and immediate scanners on files

As expected, the effect of running an immediate scan on top of the on-access scans has a significant impact on server performance. This leaves the day-to-day option of just checking incoming files as the best compromise.

### Summary

The program is easy to install and use. The Scan Wizard is a useful facility for first-time users, but will be superseded as the user gets to grips with the configuration options available from the Console program. The software provides server communication for alerts and the ability to set up servers to receive updates automatically from a defined source.

The presence of a command-line scanner provides a high level of configurability where the software has to be used in conjunction with specific program environments. This allows configurations to be preset in configuration files or to be called up from tasks defined on specific servers as the need arises.

One small negative comment about the product is its ability to handle only a single scheduled task. Administrators wanting to define multiple scheduled jobs will need to have them pre-defined and run using the *NT* scheduler. Not the end of the world, but it just takes the shine off what is otherwise a comprehensive and very user-friendly product; although as stated previously, the company states that this issue has now been resolved in version 3.0.

## NetShield for Windows NT

Detection Results

| Test-set[1] | Viruses Detected | Score |
|---|---|---|
| In the Wild File | 474/476 | 99.6% |
| In the Wild Boot | 86/87 | 98.9% |
| Standard | 488/532 | 91.7% |
| Polymorphic | 9197/11000 | 83.6% |

Overhead of On-access Scanning:

The tests show the time (in seconds) taken to copy 200 EXE and COM files (20.55MB). Each test is performed ten times, and an average is taken.

| | Time | Overhead |
|---|---|---|
| Program not loaded | 15.2 | – |
| Program unloaded | 16.3 | 7.2% |
| Program loaded: | | |
| No incoming/outgoing files, no manual scan | 19.2 | 26.3% |
| Incoming files, no outgoing files, no manual scan | 26.1 | 76.3% |
| Incoming and outgoing files, no manual scan | 28.0 | 84.2% |
| Incoming and outgoing files, manual scan | 50.6 | 232.9% |

**Technical Details**

**Product:** *NetShield for Windows NT v2.5.3a*.

**Developer/Vendor:** *McAfee Associates*, 2710 Walsh Avenue, Santa Clara CA 95051-0963, USA. Tel +1 408 988 3832, fax +1 408 653 3143.

**Distributor UK:** *McAfee UK Ltd*, Hayley House, London Road, Bracknell, Berks RG12 2TH. Tel +44 1344 304730, fax +44 1344 306902.

**Price:** US$1600.00 per 100 users (unlimited servers), including updates; monthly if downloaded from the usual sources, quarterly if shipped. Prices for larger licences on request.

**Hardware Used:** *Compaq Prolinea 590*; 80MB RAM with a 2GB hard disk, under *Windows NT 4.0* with service pack 1.

[1] Test-sets: In the Wild file, Standard, and Polymorphic; see *VB*, March 1997, p.17. For a listing of the In the Wild boot sector test-set, see *VB*, January 1997, p.17.

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:

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

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

# END NOTES AND NEWS

***Sophos Plc's* next round of anti-virus workshops** will be on 21/22 May 1997 and 9/10 July at the training suite in Abingdon, UK. The company's training team is also hosting a Practical *NetWare* Security course on 13 May 1997 and 3 July (cost £325 + VAT). Information is available from Julia Edwards, Tel +44 1235 544028, fax +44 1235 559935, or access the company's World Wide Web page; http://www.sophos.com/.

A **Web-enabled version of *Integralis' MIMEsweeper*** security software has been released. Version 3.0 of the product provides anti-virus scanning of Web, FTP, and email transmissions, plus various contact management and control features. The package is a combination of two modules, which can also be purchased separately: *MAILsweeper* (which manages email content) and *WEBsweeper* (which manages the interaction with Web and ftp). Further information available from Sue Trussler at *Integralis*; Tel +44 1189 306060, or email info@integralis.com.

*Reflex Magnetics* will be holding more of its **'Live Virus Experience'** courses, on 13/14 May 1997. Fronted by Dr David Aubrey-Jones, they will be held at the company's training room on its premises, and cost £345 for one day (Introduction), or £595 for two (Introduction and Advanced). Further security courses offered by the company, and fronted by Steve Bailey, include The Hacking Threat (20–22 May), UNIX Threats and Vulnerabilities (23 May). For information on these and other courses, contact Phillip Benge at *Reflex*; Tel +44 171 372 6666, or visit the Web site; http://www.reflex-magnetics.co.uk/.

*IBM* has launched an initiative in cooperation with *Chubb*, *Reliance National*, and Danish insurer *Codan*, **to help insurance companies evaluate the risks related to the Internet**. The companies involved believe that recent growth of the Internet indicates electronic business is rapidly becoming a major factor in the business world. The projected services will cover cyberspace losses, and the policies are expected to compensate for losses resulting from unauthorized access from, for example, hackers. *IBM* has produced a document on insuring virtual assets; 'Internet Insurance: Property, Contents, and Commerce': it can be viewed at http://www.dk.ibm.com/industry/warehous.html. *IBM Global Insurance Industry's* Internet home page can be visited at http://www.insurance.ibm.com/insur/.

*Dr Solomon's Software Ltd* is presenting **Live Virus Workshops** in the UK on 13/14 May 1997. Details are available from Melanie Swaffield at *Dr Solomon's*; Tel +44 1296 318700. The company has also announced the launch of an anti-virus product for SMTP email users, *MailGuard*. The software is designed to provide 'high-speed real-time scanning for email servers of all kinds'. Information on this and other products can be found on the company's Web site; http://www.drsolomon.com/.

***Security Workshop 1997*, this year's EICAR conference**, will be held at the University of the German Armed Forces in Hamburg, from 6–8 September 1997. The event costs DM580 (DM290 for government, NATO, and military members and for students; DM260 for EICAR members), and accommodation is available on request. For information contact the EICAR office at Hochstallerweg 28, D-86316 Friedberg, Germany; or visit its Web site; http://www.eicar.com/.

The case of **teenage hacker Richard Pryce** has finally been heard in the British Crown Courts. Pryce became infamous in 1994 when, at the age of 16, he was arrested for hacking into the computer systems of the US Air Force from a PC in his home. This resulted in his being charged with twelve offences under Section 1(1) of the Computer Misuse Act 1990. Pryce pleaded guilty: his defence of being motivated purely by youthful curiosity was accepted by the Crown, and he was ordered to pay a fine of £1200, and £250 towards costs.