ISSN 0956-9979 JANUARY 1997

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

IN THIS ISSUE:

• **Scanning for answers.** The latest in the regular biannual comparative tests for DOS and *Windows* anti-virus software is published this month. How did the field look for the 21 competitors? Turn to p.9 for the story.

• **Here a virus…** After the plethora of *Word* macro viruses seen recently, this month sees analyses of two more 'traditional' viruses: for descriptions of Hooter and WildLicker, turn to p.6 and p.7.

• **Alert to the risk.** *Look Software's Virus ALERT* has been around for a couple of years now – how is this small company faring in the cut-throat world of anti-virus software? See p.21 for an assessment.

CONTENTS

EDITORIAL

Cry 'Hoax!' and let slip the dogs of war…

In recent years, and even more so in recent months, a new type of threat has emerged. More insidious than any unseen remote attacker, more confusing than any traditional virus, more time-consuming than a total network shutdown, there is real danger of this threat becoming the major problem facing security administrators. In these days of global connectivity, where most organisations have at least some level of access to the Internet, the hoary old saying 'Information is power' combines with the Internet cliché 'Information wants to be free' with consequences perhaps best described as hazardous.

" VB is receiving more technical support calls concerning hoaxes than genuine viruses "

I refer, of course, to hoaxes. An alarming number of these have been perpetrated over the last few months, to such an extent that at the time of writing, *VB* is receiving more technical support calls concerning hoaxes than genuine viruses.

Such things are not perhaps as recent a phenomenon as one might think – as early as 1988, a BBS user going by the pseudonym 'Mike RoChenle' warned of a virus carried by 'subcarrier frequencies on 2400 baud modems'. However, this (widely disseminated at the time) pales into insignificance when compared with the all-time classic: the Good Times hoax.

Good Times, with which every reader must surely be familiar, surfaced two years ago, and still crops up intermittently, although seemingly with fewer believers each time. More recently came Irina, a slightly unusual class of hoax – the misguided publicity attempt [*see VB, October 1996, p.3*]. Even in the last two months, at least three more non-virus scares have surfaced.

The first of these was a warning stating that 'The Internet community has again been plagued by another computer virus ... this virus, referred to as Deeyenda Maddick, performs a comprehensive search on your computer, looking for valuable information such as email and login passwords, credit cards, personal inf., etc.'. Since November, queries about this have been received by anti-virus companies world-wide: whilst clearly a hoax, the humour behind the name was only recently revealed. To appreciate this, readers should read the name aloud several times in succession…

Hot on the heels of Deeyenda came PenPal (which was similar to early Good Times warnings) and Goblyn. Were these real viruses, it seems probable that both would be classified merely as Good Times variants...

However, much more interesting than the simple details of each, to my mind, are the mechanics behind them – what is it that allows hoaxes to have such an impact? A little thought leads me to conclude that it is down to one thing – the rapid expansion in the use of computers and, perhaps more immediately relevant, the Internet.

The Internet is no longer the preserve of the self-confessed computer geek: it is now a place where the newly-technologically aware Joe Public and (to an increasing extent) his family come to work and to play – in short, to communicate. This was, to a certain extent, inevitable: we computer geeks are in such a minority that we were bound to be overrun in the end; even our most treasured possession was bound to be appropriated by others…

Unfortunately, despite the fact that Joe Public is indeed technologically aware, he does not know quite enough to determine that, say, the Good Times alert he has just received from George Citizen across the country is not realistic. Poor Joe is an innocent when it comes to the inner workings of computers and their software – and this is very different from the fact that neither he nor George are familiar with the innermost workings of their TVs. These fictional people would be unlikely to believe a warning that if they watched a certain TV show all the TVs in their neighbourhood would spontaneously explode – yet when they receive the direct computer equivalent, they are convinced.

This seems unlikely to change in the near future: the speed with which PC technology is pressed upon society increases; so, therefore, does the level of public bafflement concerning what that technology can and cannot do. Indistinguishable from magic? Most definitely.

NEWS

Macro Problem with Microsofa

As *Virus Bulletin* goes to press, we learn of the discovery in the wild of a new *Excel* macro virus. *Symantec* states that the new virus was found on the western seaboard of the USA – the company's researchers have called the virus Sofa.

Unlike Laroux, which infects the *Excel* installation on a given machine by copying its macros into PERSONAL.XLS, Sofa creates a file in *Excel's* 'Alternate Startup Directory' called BOOK.XLT. This is significant, as it highlights the greater flexibility of the current versions of *Excel* (version 5 for *Windows 3.1* and version 7 for *Windows 95*) over those of *Word* as regards viruses – all *Word* viruses known currently install their macros into the file NORMAL.DOT.

The virus creates two worksheets, one with a name of twelve spaces, the other with a thirteen-space name. Both hold copies of the virus' four macros (Auto_Open, Auto_Close, Auto_Range, and Current_Open), but only one is a module: the other is a worksheet. On initial infection, a dialog is displayed reading 'Microsoft Excel has detected a corrupted add-in file. Click OK to repair this file.' If OK is selected, the virus creates the infected file BOOK.XLT. Also, the words 'Microsoft Excel' in the application's title bar are changed to read 'Microsofa Excel' when an infected file is loaded.

Whilst the virus was discovered in the wild, it has only been seen at the site where it was first found. It is not yet known how far (or if) the virus has spread beyond that location, and there is no reason to believe Sofa will become widespread ∎

Sophos Transatlantic

In mid-November, UK anti-virus vendor *Sophos Plc* opened the office of its new subsidiary company, *Sophos Inc*, in Massachusetts, USA. This follows hard on the heels of the parent company winning the *3i Quest for Growth* award [*see VB, November 1996, p.3*], and looks set to increase the battle for trade in the already cut-throat US anti-virus software market.

'The North American market is the largest and most competitive in the world,' said Richard Jacobs, President of *Sophos Inc*. 'We are here for the long term.'

Sophos Inc has announced that it will sponsor *NCSA's IVPC '97*, to take place in Washington DC on 16–17 January 1997 (speakers include *VB* editor Ian Whalley) ∎

VB '97

Virus Bulletin announces a preliminary call for papers for its next conference, *VB '97*: abstracts of approximately 100 words may be submitted to conference coordinator Alie Hothersall (fax +44 1235 531889, email ah@virusbtn.com), and should reach *VB* by Friday 31 January 1997 ∎

Prevalence Table – November 1996

Virus	Type	Incidents	Reports
Concept	Macro	180	22.2%
NPad	Macro	67	8.3%
AntiEXE.A	Boot	61	7.5%
Form.A	Boot	51	6.3%
Parity_Boot.B	Boot	42	5.2%
Wazzu	Macro	36	4.4%
Empire.Monkey.B	Boot	32	3.9%
Ripper	Boot	30	3.7%
Junkie	Multi	24	3.0%
NYB	Boot	23	2.8%
WelcomB	Boot	18	2.2%
AntiCMOS.A	Boot	17	2.1%
MDMA	Macro	17	2.1%
EXEBug	Boot	10	1.2%
Natas.4744	Multi	10	1.2%
Sampo	Boot	9	1.1%
Telefonica	Multi	8	1.0%
Imposter	Macro	7	0.9%
Jumper.B	Boot	7	0.9%
Manzon.1414	File	6	0.7%
Stoned.Angelina	Boot	6	0.7%
Tentacle	File	6	0.7%
Assistant	Macro	5	0.6%
DelCMOS.B	Boot	5	0.6%
J&M	Boot	5	0.6%
Laroux.A	Macro	5	0.6%
MtE (encrypted)	File	5	0.6%
Quandary	Boot	5	0.6%
Tequila	Multi	5	0.6%
Delwin.1759	Multi	4	0.5%
One_Half.3544	Multi	4	0.5%
Tedious	Macro	4	0.5%
TPVO.mp.3783	Multi	4	0.5%
Other [1]		93	11.5%
Total		811	100%

[1] The Table includes three reports of each of the following: Defo, Edwin, Irish, Neuroquila, Stoned.Spirit, and Unashamed.

The Table includes two reports of each of the following: Bandung, Barrotes.1310.A, Boot.437, Burglar.1150.A, Empire.Monkey.A, Feint, Helloween, Nuclear, SheHas, StealthBoot.C, Swiss_Boot, Taekwondo, Tempest, Tubo, and V-Sign.

The Table includes one report of each of the following: A&A.506, AntiEXE.C, Atomant, Bye, Byway, Colors, Cruel, Dark_Avenger.1800, Die_Hard, Dir_II.A, Face.2521, FAT_Avenger, Frankenstein, HideNowt.1741, Hot, Jerusalem, Kasiuana, KeBUG.1720, Laroux.B, Major.1644, Michelangelo, NOV17, Nutracker, Oxanna.1671, Pheew, Pindonga.4010, Purcyst, Rapi.C, Russian_Flag, Sabotage.13, Sack, Satan, Stat, Slovak.3584, Stoned.Diablo, Stoned.NoInt, Stoned.Stonehenge, TaiPan.438, Tentacle.10634, TodayJFK, Trojector.1463, Urkel, WBoot.?, Werewolf.1500.B, and Yankee_Doodle.

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 21 December 1996. Each entry consists of the virus name, its aliases (if any) and the virus type. This is followed by a short description (if available) and a 24-byte hexadecimal search pattern to detect the presence of the virus with a disk utility or a dedicated scanner which contains a user-updatable pattern library.

Type Codes

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

AD.132

CN: An appending, 132-byte, direct, fast infector containing the text: '*.com'. The virus does not infect files starting with the byte E9h (jump).

```
AD.132                  B440 B984 0090 555A CD21 B800 4233 C933 D2CD 215E 568B 441A
```

AD.157

CN: An appending, 157-byte, direct, fast infector containing the text: '*.com'. Infected files are marked with the byte ADh at offset 0003h.

```
AD.157                  B440 B99D 0090 555A CD21 B800 4233 C933 D2CD 215E 568B 441A
```

AD.173

CN: An appending, 173-byte, direct, fast infector containing the text: '*.com'. All infected files are marked with the byte ADh located at offset 0003h.

```
AD.173                  B440 B9AD 0090 555A CD21 B800 4233 C933 D2CD 215E 568B 441A
```

Amazon_Queen.484

CER: An appending, 484-byte variant containing the text: ' Amazon Queen...v1.1', 'WHY?' and 'LoRD Zer0'. Infected COM files start with character 'A' (41h) and EXE files have '0' (30h) located at offset 012h.

```
Amazon_Queen.484        0E1F E800 005D 81ED 0500 06B4 ACCD 213C 3075 132E 3B9E E001
```

AustralianParasite.209

CER: An appending, 209-byte virus which marks all infected files with byte E9h at offsets 0003h (COM) and 0012h (EXE).

```
AustralianParasite.209  40B9 D100 99CD 21B8 0042 33C9 CD21 B440 B118 BAD1 00CD 21B4
```

Bill.2658

CER: A stealth, 2658-byte virus containing a payload which triggers on the 31st of a month. The characters on screen move, change colours, and gradually disappear (billiard-like simulation). Infected files have their time-stamps set to 62 seconds.

```
Bill.2658               061E E8DC 052E C706 DE08 3300 9C58 0D00 0350 9D90 9090 9090
```

Brackets.1367

CER: An appending, 1367-byte virus which infects programs on execution or when the 'dir' command is executed. Infected files end with the word 2928h – '()'.

```
Brackets.1367           5106 B4EE CD21 81FF CC44 7503 E9A7 001E 5D4D 8EC5 8BF3 2680
```

Doglasi.1537

CER: An encrypted, appending, 1537-byte virus containing the text: 'COMSPEC=', 'BUAA is very W.C. !!!' and '——DogLasi.H'. The eighth byte from the end of infected files is set to 'E' (45h) in EXE programs or 'C' (43h) in COM programs.

```
Doglasi.1537            E800 005B 8D06 1006 2BD8 C330 1446 E2FB C38D B78F 048D BF28
```

Flowers.1688

CER: A stealth, 1688-byte virus containing the text: 'GOLDEN FLOWERS!', 'VEGERATABLES!', 'PLEASE REMEMBER239', 'C:\COMMAND.COM', 'RNL386.EXE' and 'SAE7'. All infected files have their time-stamps set to 42 seconds.

```
Flowers.1688            268B 4505 3DFB 8074 03EB 0890 268B 4507 3DFC FA07 C3B8 003D
```

Goodluck.300

CR: A prepending, 300-byte virus residing in the Interrupt Vector Table. It contains the text: '!·Good luck!'.

```
Goodluck.300            BE00 01BF 0002 B996 00F3 A58E D8BA 3B02 B821 25CD 210E 58BE
```

HV.1169

ER: An appending, 1169-byte virus containing the text: '????????EXE' and '*.EXE'. All infected files have the string 'HV' located at the end of code. The virus payload triggers on Mondays, between January and July, and displays a multi-colour, vertical, scrolling bar.

```
HV.1169                 B800 33BE 7101 BF0B 01CD 2181 FA34 1274 75E8 3003 7270 B821
```

HXH.1585

CER: A stealth, appending, 1585-byte virus containing the encrypted text: 'JFD-01'. On 19 February the virus plays the Russian tune 'Podmoskovnye Veczera' and displays (yellow on red) the text: 'HXH: Wherever,Long Live Our Friendship! Good Luck With You! My Friend. Yours Sincerly 6162910'.

```
HXH.1585                E851 05B4 FECD 2180 FCAA 7550 803E CF06 0174 2B8C C82B 062F
```

HXH.1680

CER: A stealth, polymorphic, appending, 1680-byte variant of HXH.1585. It contains the text: 'HXH: Wherever,Long Live Our Friendship! Good Luck With You! My Friend. Yours Sincerly 6162910'. Infected files have their time-stamps set to 60 seconds. The following template detects the virus in memory only.

```
HXH.1680                5BB4 FECD 2106 80FC AA75 3707 80BF D405 0174 1C8C C82B 87C3
```

IVP.Scroll.630 **EN:** An appending, 630-byte, fast, direct infector containing the text: 'The Scroll Virus!George GoulemasHello world! This is the Scroll Virus!', ''I hope you enjoy it (NOT!)', 'Ciao!', '[IVP]' and '*.exe'. All infected files are marked with the word 4747h located at offset 0010h (initial SP).
`IVP.Scroll.630      B44E B907 00CD 2172 07E8 0500 B44F EBF5 C3B8 003D E82D 01B4`

Midi.765 **CR:** An appending, 765-byte virus containing the text: 'MidInfector by Dark Slayer of [TPVO]'. The virus has an unusual way of gaining control when an infected file is executed: the near jump to virus code is not located at the start but inserted inside the original program's code. Thus, the virus is not in control until the execution flow reaches the location patched by the virus during infection.
`Midi.765            5E83 EE0E 56B8 8818 CD21 3D49 4D74 43B4 4ABB FFFF CD21 B44A`

Mman.2048 **CER:** An appending, 2048-byte virus containing the text: 'MMAND.COM'. The sum of the last and the second last words of the code in all infected files is equal to FFAAh.
`Mman.2048           B808 E7CD 213D CD12 7403 EB64 9080 3E94 00FF 7414 06FF 3695`

Mothership.655 **ER:** An appending, 655-byte virus containing the text: 'MoTHER MotherShip (c) 1994 Stormbringer'. Infected files are marked with the character 'M' at offset 0012h.
`Mothership.655      B8AD 4BCD 213D AD2B 7402 F8C3 F9C3 B42B CF3D AD4B 74F8 3D00`

Rtfishel.1574 **CER:** An appending, 1574-byte virus containing the text: '22/07/95' and 'John Galt - RT Fishel'. Infected files have their time-stamps set to 62 seconds.
`Rtfishel.1574       5E81 EED7 04B8 ED1D CD21 3DEB FE75 4C90 900E 1F81 C60E 0681`

SillyC.99 **CN:** A prepending, 99-byte, fast, direct infector containing the text: '*.cOM'. The virus does not infect files starting with byte BEh (such files are already infected).
`SillyC.99           1F8B D7B9 6300 B440 CD21 598E DEB4 40CD 21EB BFBE 6301 FA57`

SillyC.224 **CN:** An appending, 224-byte, direct infector containing the text '*.COM'. The virus does not infect files starting with byte E9h (jump).
`SillyC.224          33C9 8BD1 B802 42CD 215A B9E0 00B4 40CD 21B4 3ECD 21BA 8000`

SillyC.240 **CN:** An appending, 240-byte, fast, direct infector, containing the encrypted text: '*.com'. The virus does not infect files starting with byte E9h (jump).
`SillyC.240          B440 B9F0 008D 9603 01CD 213E 8B86 0F02 2D03 003E 8986 F301`

SillyC.358 **CN:** An appending, 358-byte, fast, direct infector containing the text: '*.com'. Infected files are marked with byte 0DDh offset 0003h.
`SillyC.358          8B4F 025B 3D4D 5A75 03EB 4D90 80FD DD75 02EB F6B8 0242 33C9`

StarDisco.223 **CN:** An overwriting, 223-byte, fast, direct infector containing the text: 'The discolored star is doing nothing in your computer Don't press any key' and '*DISCOLOREDSTAR will infect all your .COM files! HuAhUaHuA*'. Infected files are destroyed and truncated to 223 bytes.
`StarDisco.223       B440 B9DF 00BA 0001 CD21 B43E CD21 C30D 0A54 6865 2064 6973`

StarGreen.407 **CN:** An overwriting, 407-byte, fast, direct infector containing various text strings. Infected files are destroyed and truncated to 407 bytes.
`StarGreen.407       B440 B997 01BA 0001 CD21 B43E CD21 C30D 0A54 6865 2066 6C69`

Trivial.33.C **CN:** An overwriting, 33-byte, direct infector containing the string: '*.c*'. The virus infects the first file in the current directory.
`Trivial.33.C        4ECD 21BA 9E00 B801 3DCD 218B D8B4 40B1 21BA 0001 CD21 CD20`

Trivial.71 **CN:** An overwriting, 71-byte, fast, direct infector containing the string: '*.com'. Since the virus has the structure of an EXE file, all infected programs begin with: 'MZG'.
`Trivial.71          BA00 01B9 4700 B440 CD21 B43E CD21 B44F CD21 73E3 E9BF FE2A`

WeekDay.1614 **CER:** A stealth, encrypted, appending, 1614-byte virus.
`WeekDay.1614        50B8 5DDF CD16 3D49 0C58 C350 5351 B430 CD21 3C03 595B 58C3`

WhiteNoize.1602 **CER:** A stealth, appending, 1602-byte virus containing the text: '¡!¡WHiTE NOiZE!¡!', 'SMARTCHK.CPS', 'CHKLIST.MS', 'ANTI-VIR.DAT', 'A Little Mood Music' and 'courtesy of MnemoniX'. The virus waits at least two minutes after every infection before infecting a new file. The payload includes deleting the integrity data files, and sound effects. Infected files have their time-stamps set to 62 seconds.
`WhiteNoize.1602     B8AE 0BCD 2181 FE43 6574 7B8C C048 8ED8 812E 0300 8000 812E`

Wsurc.1730 **CEN:** An encrypted, prepending (COM) and appending (EXE), 1730-byte fast, direct infector containing the text: 'WSURC.DMA' and 'C:\WIN95\WRIVDR.CNF'.
`Wsurc.1730          072E 8B84 1E01 33C3 33C6 2E89 841E 0183 C602 81FE A106 72E9`

Xuxa.2058 **CER:** A stealth, encrypted, appending, 2058-virus containing the text: 'XUXA PARK 2.1 z BY HADES "Y LUCHEMOS PARA QUE TODOS LOS NIÑOS DEL MUNDO TENGAN DERECHO A SOÑAR, A SOÑAR POR IGUAL"', 'TBF-ZIRJCHKCHKLIST.MS' 'ANTI-VIR.DAT' and 'COMEXE'. Infected files have their time-stamps set to 38 seconds.
`Xuxa.2058           8DB6 3E00 8D86 2A00 E312 0E50 2E31 142E D204 46FE C249 CBFB`

VIRUS ANALYSIS 1

Hooter.4676: Yum, yum, yum!

Oleg Petrovsky
Cybec Pty

Hooter.4676 stands out from the thousands of viruses already in existence in several different ways. First, it belongs to the relatively small group of viruses written in a high level language (HLL). More remarkably, it is one of the few members of this group which have been successful in the wild – indeed, the number of reported incidents is still, at the time of writing (October/November 1996) slowly growing. Finally, the virus has an interesting method both of infecting its targets, and passing control to the original hosts.

To complete the picture, Hooter.4676 is a parasitic, prepending, direct EXE and COM infector, which infects one file at a time and contains a rather harmless payload.

Execution

The Hooter.4676 virus spreads in compressed form, so when an infected file is executed, the virus' first step is to expand its code. The compression technique used by Hooter is not reminiscent of any commonly-known algorithm (e.g. LZEXE, PKLITE, DIET, etc) but it is quite possible that it is a standard feature of the linker used by the virus author.

When decryption is complete, the virus executes the HLL's run-time start-up code. Next, it hooks all necessary interrupts and sets all necessary variables.

Then the real work begins. The virus collects information on all available disk drives (it tests everything from C: to Z:). Hooter then throws away all but the first ten entries from the newly-created list – these drives will be searched later for suitable targets. Therefore, on differently-configured systems, Hooter will infect files on different drives, and network drives are not excluded from danger.

The virus' next step is to preserve its current command-line information, so it will eventually be able to run the original host correctly before returning to the user prompt. Next, Hooter checks the first drive from the list. It determines the amount of available free disk space and skips to the next drive if that amount is less than 400K.

Otherwise, the virus performs a recursive scan of selected drives. It skips volume names, enters every subdirectory, searches for an uninfected EXE or COM file, and deletes files called 'chklist.*' and 'anti-vir.dat'.

Once the virus has found and infected one file, or encounters any DOS error, it returns control to the host file. Hooter.4676 keeps the original file encrypted, and must therefore decipher the file before executing it. To do so, the virus creates a file called 'HOOTERS.EXE', located in the same directory as the original file. Next, it accesses the infected file and, after skipping its own code, reads the original program in 4676-byte chunks, decrypts it and writes it to 'HOOTERS.EXE'.

Finally, the virus locates the current COMMAND.COM by using a COMSPEC environment variable, and launches the program HOOTERS.EXE, using its name as an argument in a newly-constructed command line (it also includes the preserved parameters from the original command line).

There are only two things left now: removal of the file HOOTERS.EXE from a disk, and a call to the payload of the virus.

Infection

Once a potential target is found, the virus checks the first byte of the file under attack. If this is 'Z' (5Ah), the file is assumed to be already infected. The virus also does not attempt to infect the file COMMAND.COM. With these exceptions, it will try to infect any other file with the extension 'EXE' or 'COM'.

To infect a new file, Hooter once again uses a temporary file, called HOOTERS.EXE, located in the same directory as the victim. Then it copies its own compressed body (4676 bytes) into this file, and attaches the encrypted host file, which it reads, encrypts and writes in 4676-byte-long blocks. Finally, it changes the name of HOOTERS.EXE to the original name of the victim and restores the original attributes and time-stamp.

One of Hooter's most important features is its wide range of potential targets. Excepting (as mentioned above) the file COMMAND.COM, and files beginning with 'Z', any file with the extension 'EXE' or 'COM' will be infected. The impact of this on non-DOS executable programs can be considered an additional payload.

Payloads

If no suitable clean targets are found, Hooter exercises one of its payloads immediately before returning to the user prompt. Depending on a value read from the internal system clock, the virus may display the following message:

```
Hooters, hooters, yum yum yum. Hooters,
hooters, on a girl that 's dumb. - Al Bundy.
```

As mentioned earlier, Hooter also deletes all 'chklist.*' and 'anti-vir.dat' files found while searching the drives. A minor flaw in the virus' logic has an interesting impact on infection operation – the virus abandons its search for any new targets as soon as it encounters a disk containing a 'chklist*' volume.

As mentioned above, another (perhaps unintentional) payload is the effect on all *Windows* (or, generally speaking, non-DOS) applications. All files infected with Hooter.4676 look like normal DOS executable programs and are treated as such when launched.

First, the system will run an infected file in its DOS mode. The virus will scan a disk and infect one file, and will then try to execute the original application and fail.

In *Windows 95* users may see the message: 'drive:\path\filename is not a valid Win32 application'. If thesame program is called from the DOS prompt, *Windows 3.11* users will see the message: 'This program requires Microsoft Windows'. Under *Windows 95*, however, the system will launch the *Windows* application with no problems whatever.

Conclusion

Although it is a DOS virus, Hooter.4676 might be yet another sign of the tendency to leave the art of assembler programming behind. As we move towards more complicated and potentially more secure operating systems (notably *Windows NT* and *Windows 95*), it is worth remembering that HLL programming is not exclusively reserved for non-malicious applications.

When viruses have to operate on higher and more sophisticated levels, we can expect to see more viruses which are written in high level languages and which are successful enough to become a problem – indeed, macro viruses are a good example of this.

Hooter

Aliases:	Hooter.4676, HLLP.4676, HLLP.Hooter.
Type:	File, parasitic, prepending, direct EXE and COM infector.
Self-recognition in Files:	
	First byte: set to 'Z' (5Ah).
Hex Pattern in Files:	
	`B81E 018C CA03 D08C C981 C17B 0151 B901 0051 0606 B1FF 518C`
Trigger (Payload):	
	Deletes files: 'chklist.*' and 'anti-vir.dat' Displays the message: 'Hooters, hooters, yum yum yum. Hooters, hooters, on a girl that 's dumb. - Al Bundy.' Text not displayed: 'Wow - you've found the hidden message (like it's hard!) Made in Auckland, New Zealand, in 1996. Contains the greatest saying of all time. Dedicated to the few truly great pairs of luscious hooters.'
Removal:	Replace infected files with clean copies.

VIRUS ANALYSIS 2

WildLicker: Hidden in PKLite

Eugene Kaspersky

'If you want to have a long life, you must have long legs,' the she-wolf teaches her cubs. 'If you want to have a long life, you must hide yourself,' the doe-hare teaches her children. 'If you want to have a long life, you must mask your code,' virus writers teach their electronic creations.

Virus writers are continually seeking new ways to enable their viruses to elude the grasp of experienced researchers, and in the process cause anti-virus developers untold anguish. The latest of their products is WildLicker, a virus named after a text string which appears in its code after it is decompressed and decrypted.

A Composite Creation

WildLicker seems to be a combination of two different engines: a virus construction kit called NRLG (NuKE Randomic Life Generator) version 0.66 and a polymorphic generator TPE (Trident Polymorphic Engine) version 1.4. The installation routine is identical to that used by NRLG-based viruses, and the virus code in the file is encrypted with the TPE polymorphic loop.

In addition to these fairly standard features, the virus conceals its code by making it look as if the file is compressed by PKLITE. The standard Jump To EntryPoint instruction usually self-evident in viruses is not present in clear in an infected file, but instead is unpacked by original PKLITE 1.15 decompression code, as placed by PKLITE at the beginning of COM files during compression.

Whereas Cruncher [*see Virus Bulletin, June 1993, p.8*] compresses the whole file, WildLicker leaves the bulk of the file uncompressed, simply compressing the entry point code and prepending the PKLITE decompression routine. As a result, the TPE decryptor is left uncompressed, but the jump to that code is hidden in PKLITE code and data. Thus, a brief glance at infected files seems to indicate that they are packed by PKLITE, nothing more.

The best way to describe WildLicker is backwards – first the infection method and then the installation routine – rather than the usual course of things (i.e. installation and interrupt hooking, then infection).

Infecting Files

When this virus attacks a file, it first allocates a block of memory to use as buffers whilst infected, hooks Int 24h to prevent the appearance of any standard DOS error messages while accessing a write-protected disk, and gets and saves the file's attributes and date/time-stamp.

To determine whether or not the file in question is already infected, the virus uses the date/time-stamp. If bit 1 and bit 3 of the seconds field are set, it assumes the file is already infected, and does not reinfect. If not, it ORs the seconds field with the value 0Ah, setting the two bits.

This stamp is left set even if the infection eventually fails, so all files accessed by the virus have a new value in the seconds field. If the virus accesses this file again, it will not even try to infect, as the file has already been accessed by the virus.

Then the virus checks the start of the file for the presence of the EXE stamp 'MZ'. If this is present, infection aborts – the virus infects only COM files. It then checks the file length; if the file is less than 512 bytes or greater than 50K in length, the infection routine terminates.

If all conditions are met, the virus moves 512 (200h) bytes from the beginning to the end of the file, then overwrites the file start with 463 (1CFh) bytes of PKLITE entry code. It then runs the TPE polymorphic engine, encrypts itself and writes the resulting encrypted data to the end of the file.

Execution

When an infected file is executed, the PKLITE entry code immediately receives control. When run, that code decompresses the routine that passes control to the virus, copies it to the beginning of the program and jumps there, just as the original PKLITE routine does.

In more detail, the 1CFh bytes which the virus saves to the beginning of the file decompress themselves to 200h bytes of data (neatly filling the gap cleared by the virus when it moved the beginning of the file during infection). These 200h bytes contain the JMP Virus_Entry (E9h XXXX) at the start, and the rest is filled with zero bytes.

Incidentally, if someone tries to decompress an infected file using a PKLITE unpacker, they will get a 200h-byte-long file with a JMP-out-of-file command at the start. From PKLITE's point of view, the file contains just 200h bytes.

This contrasts with Cruncher, where decompression of the file will reveal the virus code in clear. WildLicker defeats this approach by ensuring that manual decompression results in a corrupt file, and loss of the virus code.

Installation and Int 21h Handler

When the PKLITE entry code unpacks the data and passes control there, the JMP-virus brings control to the TPE decryption polymorphic loop. After decryption is complete, the main virus code receives control. After checking to see if it is already resident (using the standard 'Are you there?' call), the virus installs itself in memory if necessary.

It reserves a block of system memory by using the DOS calls ChangeMemory and AllocateMemory, copies its code there, hooks Int 21h, restores the program's initial 200h bytes and returns control to the now-repaired memory image of the host.

The Int 21h handler intercepts just two calls: its own 'Are you there?' call (AX=CACAh), and DOS' Load or Execute (AH=4Bh). When any file is the subject of a Load or Execute call, the virus jumps to the infection routine and infects the files, as described above.

Closing Thoughts

The virus does not manifest itself in any way and contains no more features. Like many other viruses, it is a virus with a new idea – only one new idea, but it is very new.

The virus author even remembered to thank those concerned for the use of their engines, and to 'copyright' the text:

```
3... 2... 1... WILD LICKER !!! a
PKWARE+NUKE+TRIDENT virus for your fucked
pentium (bug inside)
```

It also contains credits and the copyright messages from the original engines:

```
thanks to [NuKE] N.R.L.G. AZRAEL thanks to
PKWARE and thanks to [ MK / TridenT ] PKLITE
Copr. 1992 PKWARE Inc. All Rights ReservedNot
enough memory [TPE 1.4]
```

WildLicker

Aliases: None known.

Type: Memory-resident, polymorphic, parasitic COM file infector.

Self-recognition in Memory:
'Are you there?' call (Int 21h, AX=CACAh), returns CAh in the BH register.

Self-recognition in Files:
Bit 1 and bit 3 in seconds field of file's time-stamp set.

Hex Pattern in Files:
The virus is polymorphic, and there is no useful hex pattern. Infected files have PKLITE v1.15 entry code and a pattern at offset 01C1h from the beginning of the file, but that pattern may also be found in uninfected files. The pattern is:

```
90D0 7BE9 ???? 00FC 01EC 0103
00FF
```

Hex Pattern in Memory:

```
E80D 0AB8 CACA CD21 80FF CA74
5EB8 2135 CD21 899E C903 8C86
CB03 0E58 488E C026
```

Intercepts: Int 21h for infection.

Trigger: None.

Removal: Under clean system conditions, identify and replace infected files.

COMPARATIVE REVIEW

Faster, Stronger, Swifter

Once again, *VB* steps into the mysterious world of the DOS anti-virus product – the core technology of most anti-virus companies is to be found in their product for good old *MS-DOS*, so this review, as ever, will be concentrating very much on the scanners' technical ability.

To this end, it largely ignores going into detail on the user interface and the resulting usability of the product, and gets straight to the nitty-gritty: how quick; how reliable.

Tried and Tested

In this review, as in the last DOS comparative (July 1996), the tests were arranged so that each product was run on each sample in turn (i.e. each time it is run, the scanner is allowed to see only one infected file). Whilst this does vastly increase the time taken to run the scan tests, it is not really a problem, as each product is run automatically from batch files – human interaction is not required.

Consequently, a network of old 386 and 486 machines connected to a Pentium running a *Windows NT* server was used. The test-set was written to CD, and the *NT* server was configured to make the CD available to clients via *NT* drive-sharing. Hence, all the client machines had direct access to the samples, but there was no way that anything could modify the set.

Each sample on the CD was copied to the hard disk of the client PC, where it was scanned by the product being tested by that client. The results of the scan were recorded, and the sample deleted before the next one was copied. The log file created by each product for each sample was copied to the server as it was created.

This system, whilst not described in complete detail here, has several advantages. It allows many products to be run simultaneously against a centralised 'sample server', it minimises the opportunities for mistakes to creep in, and, for the vast majority of the time, it does not require the presence of the tester.

How the Test was Run

The In the Wild Boot Sector test-set continues to expand: for this test, it contained 86 viruses, each a live infection on its own 3.5-inch diskette.

In the last comparative review in July, an automated approach was taken to testing against boot sector viruses (an image was dropped onto a diskette, the diskette was scanned, the next image dropped, etc). This time around, the procedure has been abandoned due to the complexity of ensuring that the data gathered from such a test is accurate. Although swapping disks over 1800 times is tedious and painful, it is at least reliable.

The clean set, as always, does double duty as both a false positive and a speed test. For these, the clean files (which now number 5500 COM and EXE files spread across 121 directories and occupying 546,932,175 bytes) are placed onto a hard disk, and each product is run in turn against that disk. Clearly each product must be run under the same conditions, or the results are invalid.

One change has been introduced, to take account of the fact that a couple of products have default modes that create checksum databases of checked files. They do this so that next time they scan, they can simply compute a checksum of each file and compare it to that stored. This way, they need only scan a file if the checksum has changed since last time. Each product is therefore run twice against the clean set – both figures are given here.

The other speed tests remain unchanged: two 3.5-inch 1.44MB diskettes are used; one of which contained 43 uninfected COM/EXE files (997,023 bytes), the other containing the same 43 files, but infected with Natas (1,201,015 bytes).

Virus Test-sets

The basis for the viruses which have been designated 'in the wild' is, as usual, is Joe Wells' WildList (available at http://www.virusbtn.com/WildLists/). As the deadline for submission of products was mid-October, the WildList which was used was that dated 22 September 1996. The bid to create valid, working, checked replicants of everything on the WildList continues: this time we miss out by only four viruses which could not, for various reasons, be replicated for the test-set.

The Standard and Polymorphic sets have continued to grow over the last few months; they now number 532 and 11,000 samples respectively.

One concession in the testing methodology has been made since July: as was done in the last *NT* comparative review in March 1996, products are now explicitly asked to scan all files. This is due both to the rapid growth in the number of macro viruses in the wild, and also to the fact that scanner manufacturers do not yet agree on which file extensions should be scanned by default.

At present, there are eight *Word* viruses in the ItW test-set, each of which is represented by four samples. One of these samples is always a copy of the infected NORMAL.DOT, and the others are standard infected documents. In addition, there are four samples of the *Excel* virus Laroux.

	ItW Boot		ItW File		ItW Overall	Standard		Polymorphic	
	Number	Percent	Number	Percent	Percent	Number	Percent	Number	Percent
Alwil AVAST!	86	100.0%	431	99.0%	99.4%	532	100.0%	11000	100.0%
Cheyenne InocuLAN	83	96.5%	389	92.2%	93.9%	508	97.1%	10354	91.1%
Command F-PROT	86	100.0%	419	96.8%	98.1%	481	93.6%	6053	50.4%
Cybec VET	85	98.8%	409	94.5%	96.2%	520	98.8%	10999	98.9%
DialogueScience DrWeb	81	94.2%	425	97.8%	96.3%	519	97.8%	11000	100.0%
Dr Solomon's AVTK	86	100.0%	418	97.7%	98.7%	530	99.6%	10997	98.8%
ESaSS ThunderBYTE	84	97.7%	433	99.5%	98.8%	527	99.6%	10997	97.7%
H+BEDV AVScan	83	96.5%	409	94.2%	95.1%	509	97.1%	9636	82.7%
IBM AntiVirus	86	100.0%	425	98.6%	99.2%	527	99.2%	10998	97.7%
Intel LANDesk Virus Protect	82	95.3%	415	96.9%	96.3%	359	79.0%	10054	84.5%
Iris AntiVirus Plus	86	100.0%	428	98.4%	99.1%	517	98.3%	10366	90.0%
KAMI AVP	86	100.0%	431	99.2%	99.5%	531	99.8%	11000	100.0%
Look Software Virus ALERT	85	98.8%	431	99.0%	98.9%	532	100.0%	11000	100.0%
McAfee Scan	83	96.5%	423	97.9%	97.3%	473	93.1%	9078	77.8%
Microsoft AntiVirus	15	17.4%	94	24.0%	21.3%	189	53.4%	975	7.8%
Norman Virus Control	86	100.0%	435	100.0%	100.0%	532	100.0%	11000	100.0%
RG Software Vi-Spy	85	98.8%	416	95.2%	96.7%	484	93.9%	7731	62.9%
Sophos SWEEP	86	100.0%	431	99.2%	99.5%	526	99.2%	10998	98.9%
Stiller Integrity Master	81	94.2%	369	87.8%	90.4%	416	86.4%	3479	26.0%
Symantec Norton AntiVirus	86	100.0%	434	99.6%	99.8%	441	89.8%	10500	95.5%
Trend PC-cillin	82	95.3%	407	95.0%	95.1%	355	78.6%	9723	82.2%

Extra Tests and Scoring

As always, the workload imposed by the so-called ‘extra tests’ is completely out of proportion to the rest of the testing. These tests incorporate limited testing of the ability of the products to detect viruses live in memory, and their disinfection capabilities. For this review, the viruses used in these tests were:

- Boot: AntiEXE, Empire.Monkey.B, Form.A, NYB, Parity_Boot.B, Quandary
- File: Burglar, Manzon, One_Half.3544
- Multi-partite: Junkie

All of these tests were performed on a selection of old *Amstrad* 386 portables, with a mere 1MB of RAM [*Those were the days... Ed.*].

Disinfection of both Burglar and One_Half is considered ‘successful’ even if the file is not repaired to be completely identical to the original file. The byte at offset 12 within the EXE header is part of the checksum word – this byte is often irreparable, and is usually left by anti-virus products. However, this has no effect on the validity of the final executable file, and so is ignored here.

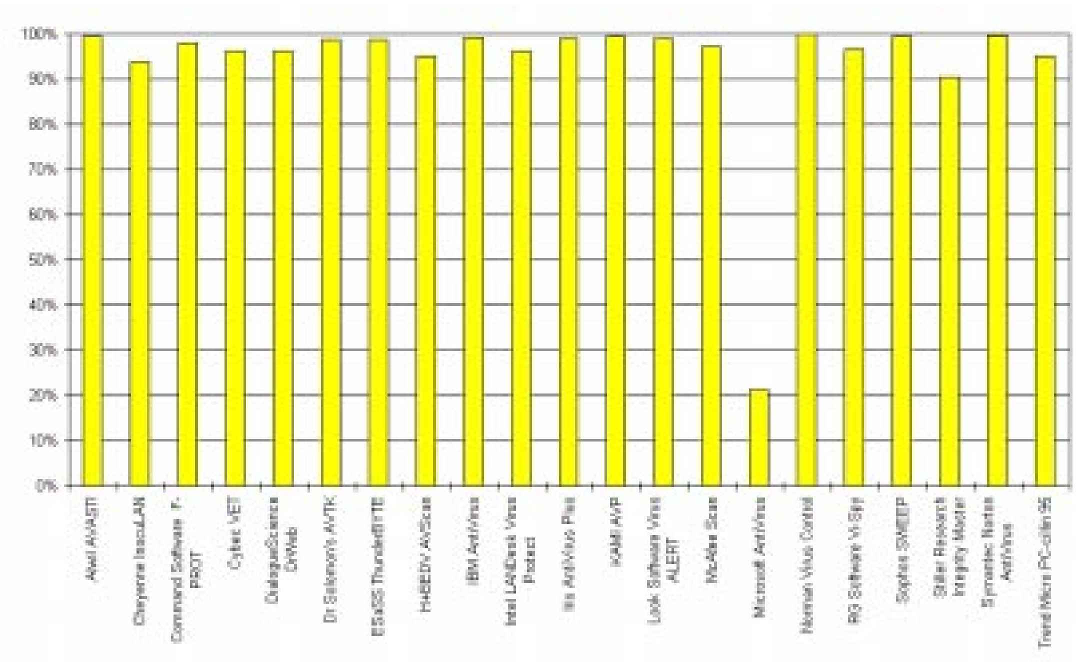
The calculation system is unchanged from the *Windows NT* comparative of October 1995 – for more information on this area, readers are advised to point the WWW browser at the document whose address is given in the Technical Details panel at the end of the article.

It is, needless to say, not possible to score the extra tests.

Alwil AVAST! v7.50-11

ItW Boot	100.0%	Standard	100.0%
ItW File	99.0%	Polymorphic	100.0%
ItW Overall	99.4%		

Results Against the In the Wild Test-set



The only samples with which *AVAST!* had trouble in this review were of Hare – two each of Hare.7610 and Hare.7750 were missed. This tiny omission drops the product to fifth in the In the Wild Overall section. Both the other test-sets were detected flawlessly. Readers may have noticed that in recent reviews, versions of *AVAST!* for other operating systems have produced 100% detection rates against all test-sets: the slight drop in the percentage score here reflects the increasing difficulty of the In the Wild set.

In the other tests, the product missed Manzon in memory, finding the other viruses without difficulty and advising the user on an appropriate course of action. As previously, *AVAST!* does not remove EXE/COM infectors, and handles boot sector virus removal by replacing the offending sector with a new, custom, boot sector (on floppies), or with a previously-saved copy of the original (on the hard disk).

Cheyenne InocuLAN v4.0j, 3.23

ItW Boot	96.5%	Standard	97.1%
ItW File	92.2%	Polymorphic	91.1%
ItW Overall	93.9%		

Notable improvement is seen here in the Standard and Polymorphic sets – both of these scores are considerably up in the last six months. Unfortunately, In the Wild scores are down by a few percent. *InocuLAN* misses 49 of the 522 samples in the combined In the Wild sets; however, the more detailed results show that the product is in fact missing identification of only twelve viruses from these sets. This is sufficient to drop the product to nineteenth (of 21) in the ItW overall category. In other tests, one result stands out: the product managed to avoid detecting Form.A in the hard disk boot sector! Such a bizarre omission cannot go unremarked, especially as the same virus was detected in the boot sector of floppy disks and live in memory. The product also seemed to hang when Junkie was active in memory: everything else was detected and disinfected in memory.

InocuLAN was able to detect and remove the viruses in the extra tests in memory, and also remove them from the other objects without problems. However, this fact is masked by the problems described. The product as it stands needs more quality assurance on the part of the manufacturer, *Cheyenne*, particularly in view of the two false positives it suffered.

Command Software F-PROT v2.24c

ItW Boot	100.0%	Standard	93.6%
ItW File	96.8%	Polymorphic	50.4%
ItW Overall	98.1%		

F-PROT again comes fairly close to attaining faultless In the Wild detection, but doesn't quite make it this time. There are several reasons for this failing: the only standard DOS viruses it misses are Digi.3547 and One_Half.3570.

However, the command-line scanner seems to have considerable trouble with *Word* macro viruses; consequently, a second executable called *F-MACRO* is provided (though not installed by default): this component performs admirably against *Word* and *Excel* viruses. One hopes that the functionalities of the two programs are combined as soon as possible, as, although users do have the capability to protect themselves against macro viruses with the current distribution, it is not obvious how to do so. The continued decline in the Polymorphic score gives cause for concern. Can it be true that *F-PROT* is third from bottom in this category?

In the extra tests, all the viruses were correctly detected in memory (in this area, a distinct improvement over performance in the last review), and all bar Manzon were removed correctly from their respective infected objects.

	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!	0:43	22.6	1:01	19.2	3:53	2292.3	3:53	2292.3
Cheyenne InocuLAN	0:41	23.7	0:39	30.1	8:29	1049.3	8:29	1049.3
Command F-PROT	0:35	27.8	0:45	26.1	4:07	2162.4	4:07	2162.4
Cybec VET	0:39	25.0	0:45	26.1	1:44	5135.7	1:44	5135.7
DialogueScience DrWeb	1:28	11.1	1:45	11.2	55:28	160.5	2:10	4108.6
Dr Solomon's AVTK	0:42	23.2	0:55	21.3	2:47	3198.3	2:47	3198.3
ESaSS ThunderBYTE	0:32	30.4	0:33	35.5	1:44	5135.7	1:44	5135.7
H+BEDV AVScan	0:49	19.9	1:11	16.5	7:01	1268.7	7:01	1268.7
IBM AntiVirus	0:50	19.5	0:55	21.3	6:56	1283.9	1:10	7630.2
Intel LANDesk Virus Protect	0:48	20.3	0:48	24.4	10:08	878.5	10:08	878.5
Iris AntiVirus Plus	0:39	25.0	0:53	22.1	11:36	767.4	11:36	767.4
KAMI AVP	0:59	16.5	0:41	28.6	24:17	366.6	24:17	366.6
Look Software Virus ALERT	0:46	21.2	1:09	17.0	3:58	2244.2	3:58	2244.2
McAfee Scan	0:38	25.6	0:35	33.5	8:46	1015.4	8:46	1015.4
Microsoft AntiVirus	0:27	36.1	0:42	27.9	3:12	2781.8	3:12	2781.8
Norman Virus Control	0:41	23.7	0:45	26.1	5:43	1557.2	5:43	1557.2
RG Software Vi-Spy	0:45	21.6	0:48	24.4	3:30	2543.4	3:30	2543.4
Sophos SWEEP	0:42	23.2	0:29	40.4	8:16	1076.8	8:16	1076.8
Stiller Integrity Master	0:50	19.5	1:26	13.6	8:57	994.6	5:45	1548.2
Symantec Norton AntiVirus	0:44	22.1	0:55	21.3	3:10	2811.1	3:10	2811.1
Trend PC-cillin	0:48	20.3	0:56	20.9	6:43	1325.3	6:43	1325.3

Cybec VET v9.13

ItW Boot	98.8%	Standard	98.8%
ItW File	94.5%	Polymorphic	98.9%
ItW Overall	96.2%		

The results against the In the Wild test-set for *VET* in this comparative are comparable, in many ways, to *F-PROT's*. *VET* too has imperfect detection of *Word* macro viruses, so ships with a second executable (*VETMACRO*) designed specifically for detection and removal of this virus type. The job is performed very well, but like *F-MACRO*, it should be integrated into the main command-line scanner. Other than macro viruses, only Karnivali.1971, the two variants of Tentacle, and Pasta were missed in the In the Wild sets.

As far as the other test-sets are concerned, *VET* performed very well, missing just one sample in the Polymorphic test-set (PeaceKeeper.B), and twelve samples of three viruses (PS-MPC.545, XQC.133, and Warchild.886) in the Standard test-set. The product is also exceptionally fast for a non-checksumming scanner, clocking in at the same speed as *ThunderBYTE*: startling by any standards.

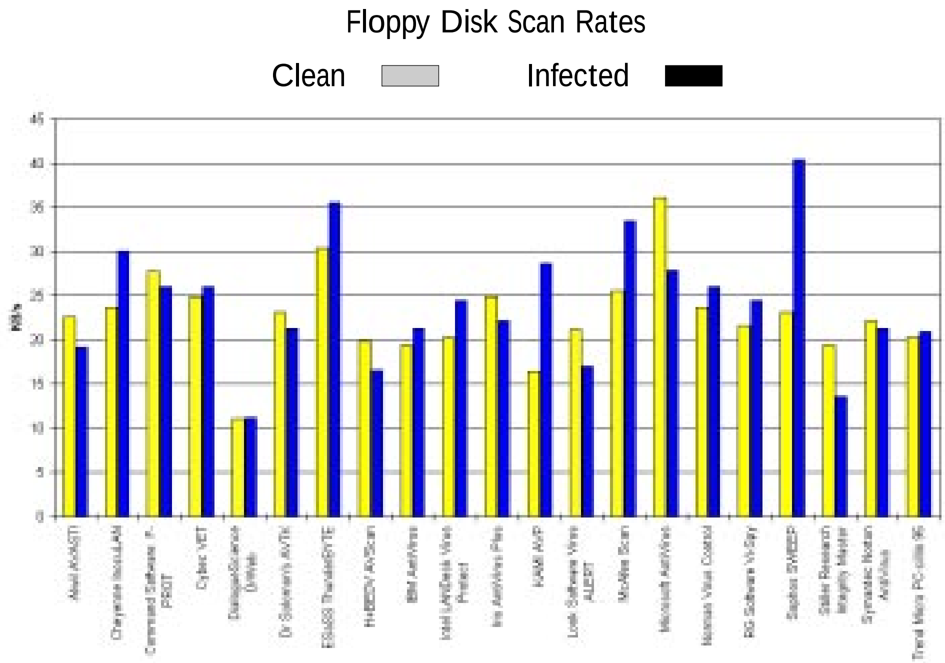
The extra tests were handled well: all viruses were detected in memory, and all bar One_Half.3544 and Manzon were disinfected. The same is true of the infected objects: all were correctly disinfected except Manzon and One_Half.3544, where disinfection was not attempted.

DialogueScience DrWeb v3.16

ItW Boot	94.2%	Standard	97.8%
ItW File	97.8%	Polymorphic	100.0%
ItW Overall	96.3%		

DrWeb is one of the comparatively few products whose speed figure when scanning a clean hard disk is different second time around. When the product is run as advised, a checksummer validates files to determine if they need to be checked again. This helps its otherwise incredibly sluggish performance: it goes from being by far the slowest product first time around to amongst the fastest on subsequent scans.

As for detection, the story is the opposite of that in the more conventional products: very good detection of the supposedly more difficult polymorphic set, but middling scores against the In the Wild sets: curious. Performance in the extra tests was excellent: all the viruses were detected and removed from all infected objects and memory. Perhaps more importantly, two false positives were encountered.



Dr Solomon's AVTK v7.63

ItW Boot	100.0%	Standard	99.6%
ItW File	97.7%	Polymorphic	98.8%
ItW Overall	98.7%		

Curiously, the distribution department at the newly-renamed *Dr Solomon's Software* shipped an outdated version of their software for this review – however, the policy is to review what is sent, which is exactly what *VB* did.

Detection in the In the Wild sets was, despite the slip-up, very good: the *Toolkit* only missed three viruses (17 samples in total, of Hare.7786, Laroux, and Xuxa.1984) in these groups. Standard (two samples of Positron were missed) and Polymorphic (three of Anarchy.6503) detection was similarly good.

On top of this, the product continues to perform well above average in the speed tests, and extremely well in the extra tests. Here, all viruses were found in memory, and disinfected from all on-disk objects.

ESaSS ThunderBYTE v7.06

ItW Boot	97.7%	Standard	99.6%
ItW File	99.5%	Polymorphic	97.7%
ItW Overall	98.8%		

TB's speed is undiminished (it seems that *Cybec's VET* has been getting faster, rather than *ThunderBYTE* getting slower…), and the detection rate is on the way up in all but the In the Wild sets. That last result is slightly unfortunate, and must surely be a measure of the ever-increasing difficulty of detecting everything out there in the real world. Only four were missed in this case: one each of Date, Hare.7750, Moloch and Werewolf.1500.B.

All viruses except Burglar were detected in memory, and all boot sector viruses correctly removed from floppy and hard disks. The product takes a somewhat unusual approach to parasitic virus disinfection, using checksum and header data on each file to aid in the attempted reconstruction of the file in question. The technique enabled it to repair successfully infections by Burglar, Junkie, and Manzon, although the disinfected Burglar file had more differences from its original than that of other products.

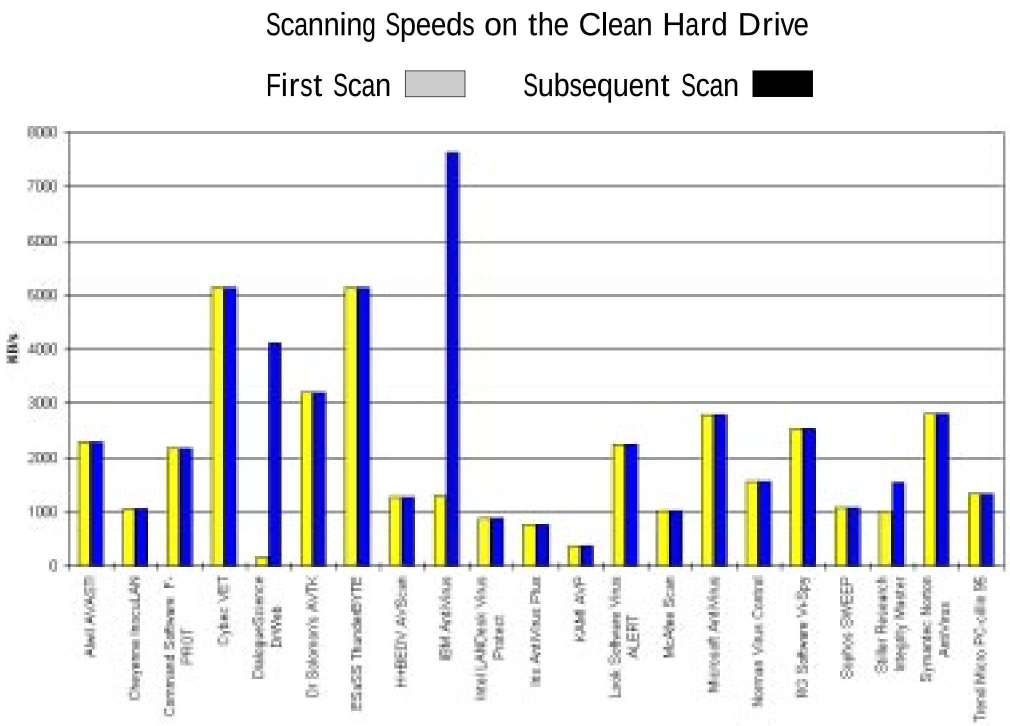
H+BEDV AVScan v3.06

ItW Boot	96.5%	Standard	97.1%
ItW File	94.2%	Polymorphic	82.7%
ItW Overall	95.1%		

Another improved performance from the German company *H+BEDV's AVScan* – scores are up again from the last comparative. Nonetheless, whilst it is improving, performance on the In the Wild sets is still weak, and there were two false positives. In the extra tests, *AVScan* detected all the test viruses in memory, but once again a version capable of disinfection was not submitted for review.

IBM AntiVirus v2.5.1

ItW Boot	100.0%	Standard	99.2%
ItW File	98.6%	Polymorphic	97.7%
ItW Overall	99.2%		



improving for a while now, but still has a little way to go, missing as it does some variants of Hare, in addition to the samples of Pieck.4444 and Xuxa.1984.

In the extra tests, *LANDesk Virus Protect* missed One_Half.3544 and Manzon in memory. All of the boot sector viruses were correctly disinfected from floppy and from hard disks, and disinfection was attempted for all file samples, but Burglar could not be run after disinfection.

Despite being a product that (at least in the UK) gets little marketing push, *IBM AntiVirus* has performed consistently over the years, and still manages to maintain the best and most far-sighted research department in the business. That department has been busy in recent months: Hare.7750 and Tentacle.10634 were the only viruses in the In the Wild test-sets for which detection was lacking.

The scores in the other test-sets are up on last time as well: the Polymorphic score, for example, is marred only by two missed samples – one each of One_Half.3544 and SMEG_v0.3. The product's speed figures are also greatly helped by being given a second shot at the clean hard drive: the checksum database built up the first time around means that the product suddenly becomes the fastest in this, more realistic, test.

In the extra tests, all viruses were detected in memory without difficulty, and all the boot sector viruses were removed from both hard and floppy disks. As for infected files, only Junkie could be cleaned.

Intel LANDesk Virus Protect v193

ItW Boot	95.3%	Standard	79.0%
ItW File	96.9%	Polymorphic	84.5%
ItW Overall	96.3%		

These tests, which were performed on the DOS component of *Intel's* essentially network-oriented solution, reveal scores which are generally unremarkable in most aspects: the detection rate against the In the Wild test-set has been

Iris AntiVirus Plus v21.24

ItW Boot	100.0%	Standard	98.3%
ItW File	98.4%	Polymorphic	90.0%
ItW Overall	99.1%		

Iris' scores continue to rise as time progresses – for a largely unknown product, it is doing well. It missed Goldbug and Tentacle.10634 in the In the Wild test-sets, and various samples from the other two groupings.

In the extra tests, all viruses were detected and disinfected from their respective objects, and from memory – a fine performance. Although thirty-two bytes were left at the end of the Manzon sample, its file header was correctly repaired.

KAMI AVP v2.2 (13/10/96)

ItW Boot	100.0%	Standard	99.8%
ItW File	99.2%	Polymorphic	100.0%
ItW Overall	99.5%		

AVP, once unbeatable in terms of detection, does not attain that level of perfection in this review. However, the product only missed the four Laroux samples in both of the In the Wild test-sets, and one of Positron in the Standard set – everything else was detected. This places the product joint third in the In the Wild rankings.

In the extra tests, all viruses except Manzon were detected and disinfected in memory, and everything was correctly removed from all infected objects on disk.

In terms of speed, *AVP* still reigns supreme: in its default configuration, *AVP* was the slowest product to run across the clean hard disk. Still, the detection rates it offers are such that under some circumstances this would be acceptable, were it not for the six false positives.

Look Software Virus ALERT v4.10 (29/09/96)

ItW Boot	98.8%	Standard	100.0%
ItW File	99.0%	Polymorphic	100.0%
ItW Overall	98.9%		

It is only in the ItW test-sets that *Look's* product does not get 100% – this mars an otherwise excellent performance. Having said that, the only samples missed in these sets were those of Hare; an omission which appears eminently fixable.

Virus ALERT detected all viruses used in the extra tests in memory, with the exception of Manzon. The boot sector samples could be removed from hard disks with the help of a recovery diskette, and the boot sectors of infected floppy disks were replaced without problems.

McAfee Scan v2.5.2, 9610

ItW Boot	96.5%	Standard	93.1%
ItW File	97.9%	Polymorphic	77.8%
ItW Overall	97.3%		

McAfee's In the Wild detection score is down since the last comparative. The fact that it missed samples of Laroux, One_Half.3570 and Xuxa.1984 in these groups is sufficient to drop it to the middle of the field. Detection in other sets is up, however, and the situation is far from irretrievable. In the extra tests, *Scan* detected all viruses used in memory, and disinfected them from all infected objects. A pleasing result.

Microsoft AntiVirus v6.22

ItW Boot	17.4%	Standard	53.4%
ItW File	24.0%	Polymorphic	7.8%
ItW Overall	21.3%		

This product is really only included to give a little light relief during testing – besides, it's nice to have a product which can be criticised for every aspect of its operation, and no one minds… Please, home users who have DOS-based machines: there are plenty of freeware/shareware products (not to mention evaluation versions) to be found on the Internet. There's no need to rely on this sort of thing.

Norman Virus Control v3.53, 2.32

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

Norman Virus Control has improved in all areas since the last test, and this time around is the only product to score 100% In the Wild detection. As well as perfect scores in all test-sets, it encountered no false positives.

Material for complaint is also reasonably scarce in the extra tests, although *Norman Virus Control* failed to detect both Junkie and Manzon in memory. Manzon and One_Half.3544 could not be removed from infected files, but everything else was handled admirably. If one had to criticise, one could always mention that it's not the fastest product around, but then the same is true for almost all the other products under test…

RG Software Vi-Spy v14.3

ItW Boot	98.8%	Standard	93.9%
ItW File	95.2%	Polymorphic	62.9%
ItW Overall	96.7%		

An all-round rise in detection rates for *Vi-Spy*, which is gratifying to see. Detection in the In the Wild set is somewhat disappointing, but this is easily remedied – as with many other products, it is basically only the more recent samples which are missed. In the other test-sets the scores are generally unremarkable.

All the viruses tested for in memory were found and identified by the product, which then advised on an appropriate course of action for each one. The boot sector viruses were correctly removed from hard and floppy disks, and Junkie and One_Half from files.

Sophos SWEEP v2.90

ItW Boot	100.0%	Standard	99.2%
ItW File	99.2%	Polymorphic	98.9%
ItW Overall	99.5%		

A good improvement against the In the Wild test-set over the results in the last comparative help to raise *SWEEP's* all-round performance: this time it only missed the samples of Tentacle.10634. In the Polymorphic test-set, the simple omission of two samples of Code.3952:VICE.05 knocks 1.1% off the score.

In the extra tests, *SWEEP* successfully disinfected all of the boot sector viruses from hard and floppy disks, with the sole exception of Junkie. As with the last comparative review, this product encountered memory problems when attempting to disinfect Empire.Monkey.B – *SWEEP* could, however, accomplish the task when copied to a write-enabled floppy disk and run from there.

The problem has to do with the minimal amount of memory on the *Amstrad* machines which were used for testing. On any more modern machine there will be no problem, as much more memory is usually available.

Stiller Research Integrity Master v3.02a

ItW Boot	94.2%	Standard	86.4%
ItW File	87.8%	Polymorphic	26.0%
ItW Overall	90.4%		

As in the last review, *Integrity Master's* In the Wild score is still too low for comfort: indeed, detection rates overall are down on last time. Users should, of course, bear in mind that *Integrity Master* is much more than just a scanner; however, the fact that a scanner is provided should stand for something.

In the extra testing, all viruses used were found in memory, and appropriate advice offered to the user. Also, all boot sector viruses were correctly removed from hard and floppy disks. Disinfection of parasitic viruses is not supported.

Symantec Norton AntiVirus v3.10

ItW Boot	100.0%	Standard	89.8%
ItW File	99.6%	Polymorphic	95.5%
ItW Overall	99.8%		

Somewhat of an ugly-duckling-to-swan transformation for this product, it would seem: in this review, it clocks very close to the top of the heap in terms of the In the Wild detection rates; a very impressive performance. Indeed, the only sample missed in either ItW set was one of the two samples of Desperado.1403.C.

Scores in the other test-sets are perhaps a little less inspiring: it is clear that *Symantec* is concentrating on the immediate threat, and dealing with In the Wild viruses as a priority.

Trend Micro PC-cillin 95 v5.02, 181

ItW Boot	95.3%	Standard	78.6%
ItW File	95.0%	Polymorphic	82.2%
ItW Overall	95.1%		

Trend's scores stay very much the same this time around. The In the Wild score is clearly the one requiring the most attention, as it places the product joint seventeenth. Missing a Jerusalem variant, for example, is not particularly good.

Extra testing provided interesting results as well: the Burglar sample, like that of *Intel*, could not be run after disinfection (this is unsurprising, as the two products use the same engine). In addition, Manzon was missed in memory, though everything else was detected while active. Everything but Burglar was disinfected correctly.

Conclusions

As usual, the frankly startling amount of data generated by this type of comparative has, of necessity, been compressed for publication. No magazine is big enough to contain the complete, detailed results for every product – and no reader interested enough to read them all anyway. The access database used to store and modify the data, and perform the complex and time-consuming calculations involved, has expanded beyond belief.

However, out of all this information there comes a pleasing general picture of the current state of anti-virus product performance. This, at the very highest level, shows us that detection of In the Wild viruses is improving, and appreciably so. For every product (*MSAV* does not count!) to score over 90% in this category is a fine sight to see, all the more so after the considerable difficulty of introducing detection for *Word* macro viruses.

Having said that, for only one product to get 100% is not quite so inspiring – it is noticeable that many products are certified by one or other (often both) of the two certification schemes out there that only pass the product if it gets 100% on In the Wild viruses. These products do not pass the same test in this review.

False Positives

Overall, the false positive results are improved since the last comparative – the complete results in this area were:

DialogueScience DrWeb	19
RG Software Vi-Spy	9
KAMI AVP	6
Cheyenne InocuLAN	2
H+BEDV AVScan	2
Intel LANDesk	1
Stiller Integrity Master	1
Trend PC-cillin 95	1

Products not listed did not encounter false positives on the collection of clean files used.

Speed

As always, the speed figures invite a variety of different interpretations; however, in terms of raw hard disk scanning speed, it is clear that *Cybec's VET* and *ESaSS' ThunderBYTE* tie for the lead. Once the second scan is taken into account, *IBM AntiVirus* streaks into the lead thanks to an extremely fast checksumming system.

The floppy scan speeds offer the usual intriguing split between those products that run faster on a clean disk, and those that run faster when the disk is infected.

In Closing

One product stands alone in this version of the DOS scanner comparative – *Norman Virus Control* was the only one to score 100% over the In the Wild sets, and it even managed it in the other sets as well. The only slight gripe is the apparent reluctance to detect Junkie and Manzon in memory, but the other test results were very good indeed.

In the Wild Boot Sector Test-set. 86 samples of 86 viruses, one sample each of:

15_Years, AntiCMOS.A, AntiCMOS.B, AntiEXE.A, Boot.437, Brasil, BootEXE.451, Bye, Chance.B, Chinese Fish, Crazy_Boot, Da_Boys, DelCMOS.B, Den_Zuko.2.A, Diablo_Boot, Disk_Killer, DiskWasher.A, Empire.Int_10.B, Empire.Monkey.A, Empire.Monkey.B, EXEBug.A, EXEBug.C, EXEBug.Hooker, Flame, Finnish_Sprayer, Form.A, Form.C, Form.D, Frankenstein, FAT Avenger, Galicia, Hare.7750, Ibex, Int40, J&M, Joshi.A, Jumper.A, Jumper.B, Junkie, Kampana.A, Leandro, Michelangelo.A, Mongolian_Boot, Moloch, Music_Bug, Neuroquila, Natas.4744, NYB, Parity_Boot.A, Parity_Boot.B, Pasta, Peter, QRry, Quiver, Quandary, 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.Dinamo, Stoned.Daniela, Stoned.No_Int.A, Stoned.June_4th.A, Stoned.Kiev, Stoned.LZR, Stoned.Manitoba, Stoned.NOP, Stoned.Spirit, Stoned.Standard.A, Stoned.Swedish_Disaster, Stoned.W-Boot.A, Swiss_Boot, Unashamed, Urkel, V-Sign, WelcomB, Wxyc.

In the Wild File Test-set. 435 samples of 125 viruses, made up of:

Anticad.4096.Mozart (4), Alfons.1344 (5), Arianna.3375 (4), Avispa.D (2), Barrotes.1310.A (2), Backformat.2000.A (1), Bad_Sectors.3428 (5), BootEXE.451 (3), Burglar.1150.A (3), Byway.A (1), Byway.B (1), Cascade.1701.A (3), Cascade.1704.A (3), Cawber (3), Chaos.1241 (6), Chill (1), Changsa.A (5), Concept (4), Cordobes.3334 (3), CPW.1527 (4), Dark_Avenger.1800.A (3), Date (4), Delta.1163 (6), Desperado.1403.C (2), Digi.3547 (5), Die_Hard (2), Dir_II.A (1), DR&ET.1710 (3), DelWin.1759 (3), Fairz (6), Fichv.2_1 (3), Flip.2153 (2), Flip.2343 (6), Freddy_Krueger (3), Frodo.Frodo.A (4), Green_Caterpillar.1575.A (3), Ginger.2774 (2), Goldbug (3), Hare.7610 (2), Hare.7750 (8), Hare.7786 (9), Helloween.1376.A (6), Hi.460 (3), Hidenowt (6), HLLC.Even_Beeper.B (3), Hot (4), Imposter (4), Istanbul.1349 (6), Jerusalem.1244 (6), Jerusalem.1500 (3), Jerusalem.1808.Standard (2), Jerusalem.Mummy.1364.A (3), Jerusalem.Sunday.A (2), Jerusalem.Zero_Time.Australian.A (3), Jos.1000 (3), Junkie (1), Kaos4 (6), Karnivali.1971 (3), Keypress.1232.A (2), Laroux (4), Liberty.2857.A (2), Lemming.2160 (5), Little_Red.1465 (2), Macgyver.2803 (3), Maltese_Amoeba (3), Mange_Tout.1099 (4), Manzon (2), MDMA (4), Mirea.1788 (2), Major.1644 (3), Markt.1533 (3), Nightfall.4518.B (2), Necros.1164 (2), No_Frills.No_Frills.843 (2), No_Frills.Dudley (2), Nomenklatura.A (6), Nop (4), Npox.963.A (2), Natas.4744 (5), Nuclear.B (4), 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), Predator.2448 (2), Quicksilver.1376 (1), Reverse.948 (3), Sarampo.1371 (6), SatanBug.5000.A (2), Sayha (5), Screaming_Fist.II.696 (6), Sibylle (3), Sleep_Walker.1266 (3), SVC.3103.A (2), Tanpro.524 (6), Tentacle (3), Tentacle.10634 (4), Tequila.A (3), Teraz.2717 (5), Trojector.1463 (6), Trojector.1561 (3), Tai-Pan.438 (3), Tai-Pan.666 (2), Tremor.4000.A (6), Trakia.653 (3), Three_Tunes.1784 (6), Unsnared.814 (3), Vampiro (2), Vacsina.TP-16.A (1), Vacsina.TP-05.A (2), Vienna.648.Reboot.A (3), Vinchuca (3), VLamix (3), Wazzu (4), Werewolf.1500.B (3), Xeram.1664 (4), Xuxa.1984 (6), Yankee_Doodle.TP-39 (5), Yankee_Doodle.TP-44.A (5), Yankee_Doodle.XPEH.4928 (2).

Standard Test-set. 532 samples of 257 viruses, made up of:

Anticad.4096.A (4), Abbas.5660 (5), Accept.3773 (5), AIDS (1), AIDS-II (1), 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), AntiGus.1570 (3), Anthrax (1), Anti-Pascal (5), Argyle (1), Armagedon.1079.A (1), Assassin.4834 (3), Attention.A (1), Auspar.990 (3), Baba.356 (2), Barrotes.840 (3), Backfont.905 (1), Bebe.1004 (1), Big_Bang.346 (1), Billy.836 (3), BlackAdder.1015 (6), Black_Monday.1055 (2), Blood (1), Blue_Nine.925.A (3), Bosnia:TPE.1_4 (5), Burger.405.A (1), Burger (3), Butterfly.302.A (1), BW.Mayberry.499 (3), BW.Mayberry.604 (6), Cascade.1704.D (3), Cantando.857 (3), Casper (1), Catherine.1365 (3), CeCe.1998 (6), Cascade.1701.Jo-Jo.A (1), Cliff.1313 (3), CLI&HLT.1345 (6), Coffeeshop (2), Continua.502.B (3), Cosenza.3205 (2), Coyote.1103 (3), Cruncher (2), Crazy_Frog.1477 (3), Crazy_Lord.437 (2), Cybercide.2299 (3), Dark_Avenger.1449 (2), Dark_Avenger.2100.A (2), Danish_Tiny.163.A (1), Danish_Tiny.333.A (1), Datacrime_II (2), Datacrime (2), DBF.1046 (2), Dei.1780 (4), Despair.633 (3), Diamond.1024.B (1), Dir.691 (1), DOSHunter.483 (1), DotEater.A (1), Dark_Revenge.1024 (3), Destructor.A (1), Datalock.920.A (3), Ear.405 (3), Eddie-2.651.A (3), Enola Gay.1883 (4), Eight_Tunes.1971.A (1), Fellowship (1), Fax_Free.1536.Topo.A (1), Finnish.357 (2), Flash.688.A (1), Feltan.565 (3), Four Seasons.1534 (3), Frodo.3584.A (2), Fisher.1100 (1), Fumble.867.A (1), F-You.417.A (1), Genesis.226 (1), Green.1036 (6), Greets.3000 (3), Greetings.297 (2), HLLC.Halley (1), Hamme.1203 (6), HDZZ.566 (3), Helga.666 (2), HLLC.Even_Beeper.A (1), HLLP.5000 (5), HLLP.7000 (5), Halloechen.2011.A (3), Horsa.1185 (3), Happy_New_Year.1600.A (1), Hymn.1865.A (2), Hymn.1962.A (2), Hymn.2144 (2), Hypervisor.3128 (5), Ibqqz.562 (3), Icelandic.848.A (1), Immortal.2185 (2), Invisible.2926 (2), Internal.1381 (1), Itavir.3443 (1), Jerusalem.1607 (3), John.1962 (3), Joker (1), Jerusalem.1808.CT.A (4), Jerusalem.Fu_Manchu.B (2), Jerusalem.PcVrsDs (4), July_13th.1201 (1), June_16th.879 (1), Kamikaze (1), Kela.b.2018 (3), Kemerovo.257.A (1), Kranz.255 (3), Kukac.488 (1), Keypress.1280 (6), Leda.820 (3), Lehigh.555.A (1), Leapfrog.A (1), Liberty.2857.A (5), Liberty.2857.D (2), Loren.1387 (2), LoveChild.488 (1), Little_Brother.307 (1), Lutil.591 (3), Maresme.1062 (3), Metabolis.1173 (3), Mickie.1100 (3), Necropolis.1963.A (1), Nina.A (1), NRLG.1038 (3), NutCracker.3500.D (5), November_17th.768.A (2), Omud.512 (1), On_64 (1), Oropax.A (1), Parity.A (1), Peanut (1), Perfume.765.A (1), Phantom1 (2), Pitch.593 (1), Piter.A (2), Pixel.847.Hello (2), Pizelun (4), Plague.2647 (2), Phoenix.800 (1), Pojer.4028 (2), Poison.2436 (1), Positron (2), Prudents.1205.A (1), PS-MPC.227 (3), PS-MPC.545 (6), Power_Pump.1 (1), Quark.A (1), Red_Diavolyata.830.A (1), Revenge.1127 (1), Riihi.132 (1), Rmc.1551 (4), Rogue.1208 (6), Saturday_14th.669.A (1), SVC.1689.A (2), Screaming_Fist.927 (4), SillyCR.710 (3), Screen+1.948.A (1), Stardot.789.A (6), Stardot.789.D (2), 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), Spanz.639 (2), Starship (5), Subliminal (1), Suomi.1008.A (1), Suriv_2.B (1), Suriv_1.April_1st.A (1), Surprise.1318 (1), Svir.512 (1), Svin.252 (3), SysLock.3551.H (2), Sylvia.1332.A (1), TenBytes.1451.A (1), Terror.1085 (1), Thanksgiving.1253 (1), The_Rat (1), Tiny.133 (1), Tiny.134 (1), Tiny.138 (1), Tiny.143 (1), Tiny.154 (1), Tiny.156 (1), Tiny.159 (1), Tiny.160 (1), Tiny.167 (1), Tiny.188 (1), Tiny.198 (1), Todor.1993 (2), Traceback.3066.A (2), TUQ.453 (1), Untimely.666 (3), V2P6 (1), Vbasic.5120.A (1), VCS1077.M (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), Vcomm.637.A (2), VFSI (1), Vienna.583.A (1), Vienna.623.A (1), Vienna.648.Lisbon.A (1), Victor (1), Vienna.Bua (3), Vienna.Monxla.A (1), Virus-101 (1), Virus-90 (1), Virogen.Pinworm (6), Vienna.W-13.507.B (1), Vienna.W-13.534.A (1), Vienna.W-13.600 (3), Voronezh.600.A (1), Voronezh.1600.A (2), VP (1), V2Px.1260 (1), Warchild.886 (3), Warrior.1024 (1), Whale (1), Willow.1870 (1), WinVir (1), WW.217.A (1), XQG.133 (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), Zherkov.1023.A (1), Zero_Bug.1536.A (1).

Polymorphic Test-set. 11,000 samples; 500 each of the following 22 viruses:

Alive.4000, Anarchy.6503, Code.3952:VICE.05, Cordobes.3334, Digi.3547, DSCE.Demo, Girafe:TPE, Gripe.1985, Groove and Coffee_Shop, 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, Uruguay.4.

PRODUCT REVIEW 1

Norton AV 2.0 for Windows NT

Martyn Perry

Norton AntiVirus for NT v2.0 (*NAVNT*) is the latest in a long line of products from *Symantec Corporation*. The product is advertised as working on *Windows NT* Workstations and Servers, v3.51 and v4.0; the review was performed on v3.51.

Licence Considerations

The licence is granted on a per-PC basis. Home use is also allowed under the terms of the agreement, provided that the PC for which the software was licensed has 80% of the total usage. The registration card must be returned to *Symantec* for the licence to come into effect.

An additional clause, which is new to me, permits a licensed user to pass previous versions to a nominated charity. This flash of altruism helps overcome the problem of users having old versions of software they are no longer licensed to use. That most software licences do not allow multiple versions of the same product to coexist on the same computer is a fact many users may not appreciate.

Presentation and Installation

Although the evaluation set came only with a pre-release hard copy of the manual, this accurately reflected the options available. The software is supplied on CD-ROM and occupies two main directories, MANUAL and NAVNT.

MANUAL contains an *Acrobat* reader and the manual in PDF format. It installs as default to C:\ACROREAD and the 101-page document takes up just under 2.5MB of space.

The installation is performed from the CD-ROM by executing SETUP.EXE in the root directory. If the CD is loaded into a system running *Windows NT v4.0*, AutoPlay will execute this automatically. Otherwise, the user must define:

- a default directory to store *NAVNT* files; the default setting is NAVNT
- initial settings – the defaults are for scheduled weekly scanning on Friday nights and for the automatic start of auto-protect

These settings are confirmed along with the location of *Symantec* shared files (the default for which is a directory called SYMANTEC).

There was a burst of activity when the directories were created and the files copied. Progress was shown by a progress meter for the overall installation. This was followed by contact information for support and the option to register for United States, Canada and Mexico only.

The installation culminated with the option to choose whether or not to perform an immediate scan. This last option I find very useful, since it allows control of the settings of the scanner before the initial run.

Component Parts

There are two main components of the product; NAVNT and Auto-Protect. NAVNT is the immediate and scheduled scanner, while Auto-Protect, the on-access component, gives continuous protection by scanning files as they are used.

If the default choice of automatically setting Auto-Protect is used, it is shown on the screen as a minimised icon. If this is selected, the Auto-Protect menu appears with the choice of minimising the application, disabling it or changing the options. Selecting Options invokes the Auto-Protect settings dialog.

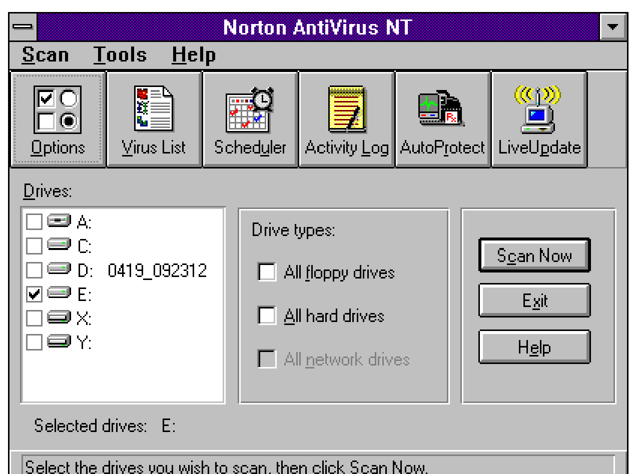
The NAVNT scanner is selected from the *NAV* program group. This starts the GUI to the various available options available for scanner management. An alternative method of running NAVNT allows the user to override configuration settings using the following command-line syntax:

```
NAVNWT [pathname] [options]
```

where pathname is any drive, directory, file or combination thereof. The options can define subdirectories, boot records and local or network drives for scanning. This type of execution is very useful if scheduled scans, needing a greater degree of selectivity than the internal scheduler, are required.

Administration

No additional password is required to access the scanner administration settings. This gives access to the various tools for drive selection.



The front-end of *NAVNT* retains the traditional look and feel of the previous *Windows* versions of the product, but masks its increased functionality.

The Virus List in the evaluation version (dated 2 October 1996), displayed information on 8186 viruses. A filter allows the user to select specific virus types – program, boot, macro etc. Individual entries in the list can be selected to provide additional detail on the characteristics of a particular virus.

The scheduler sets up a timed scan. This scans all hard drives and is limited to a single scan at a selected time on a chosen day each week. There is an option to reduce the scan speed if the server load exceeds a user-defined level (the default is 1%). If other choices are required, the scheduler must be used to execute the scanner with appropriate command-line options.

The Activity Log can be modified to display information about all server activity, or limited to activity of one type or another – virus detected, scan interrupted, etc, with a date/time stamp for each. This log file can have its size limited – the default value for this is 50KB.

Auto-Protect gives access to the Auto-Protect options menu and allows automatic protection to be enabled/disabled. The options allow the same file types, etc, to be selected as for the main scanner. 'LiveUpdate' allows updates to the virus list to be downloaded from the Internet, and 'Options' gives access to the scanner configuration settings. Options include file types, areas to be scanned, response to detected virus, alerts, general settings, exclusions, and activity logs.

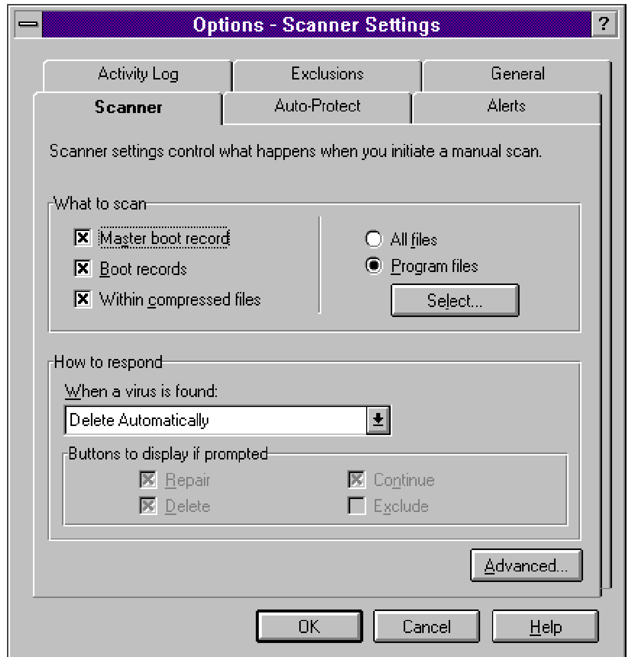
All files, or program files only, can be selected. Under program files, the default extensions to be scanned are 386, BIN, CLA, COM, CPL, DLL, DOC, DOT, DRV, EXE, NCP, NED, NNL, OCX, OV?, SCR, VBX, VXD and XL? Areas which may be scanned include boot records, master boot records and within compressed files.

Extra available options show network drives for drive selection from the main window, allow scanning to be stopped, and provide immediate notification during a scan, rather than only at the end. If this last option is selected and a virus is found, a response has to be entered before continuing the scan. If it is not selected, the infected file is either repaired or deleted, according to the configuration.

Further options are available defining the default response on detection of a virus: Prompt, which creates buttons to determine further action, Notify only, Repair automatically, and Delete automatically.

The alerts allow a warning message to be created, with the option of an additional audible alert. There is a further option which can alert the *NAV* NLM, if it is available. An option also exists to remove the alert dialog after a predetermined number of seconds.

The General settings give the file extension for backup files prior to repair – the default extension is VIR, and exclusions define files which are not to be scanned. The default entry here is *.VI?. This is useful as it avoids a scanner rechecking a group of files already tagged as infected.



NAVNT options are configured via one of the now ubiquitous tabbed dialog boxes.

The Activity Log determines which events are recorded. The default settings log known virus detections and scan completions. There is a further option to log virus list changes.

While a scan is running, a progress meter shows which file is currently being scanned. There are separate running totals for the number of files scanned, infected and cleaned. If a virus is detected during the scan, the Repair Wizard is displayed with a list of viruses detected and the choice of removing the listed viruses manually or automatically.

Updates

Updates to the virus database are free for the life of the product, and can be obtained through the automated Internet link within the product or manually from various sources: Internet, *Symantec* BBS, *CompuServe*, etc.

Updates take the form of a single file called mmNAVyy.EXE, where mm denotes the month and yy the year. When this is run, it will search the PC for copies of *Norton AntiVirus*, and the new virus definitions will overwrite the extant ones. The new set is thus available when a scan is next performed. Auto-Protect will detect the presence of the new definitions and will load them automatically.

Detection Rates

The scanner, based on the definitions dated 2 October 1996, was checked using the usual four test-sets: In the Wild File, In the Wild Boot Sector, Standard and Polymorphic (see the summary table for details). The tests were conducted using the default scanner file extensions supplied. The scanner was configured to remove infected files, and the residual file count was then used to determine the detection rate.

The results were excellent; the Polymorphic score clocked in at 100%. The In the Wild test was also impressive: only one sample (Desperado.1403.C) was missed. Although the scanner detected Dir II.A and the two variants of Byway, it was not able to remove them, despite the fact that no attributes were set on these files. [*This is actually not illogical, as the viruses in question are so-called link viruses, simple deletion of which will often leave the user with problems. Ed.*] The only slight disappointment was the run against the Standard test-set, where the score managed to reach only 82%.

Real-time Scanning Overhead

To determine the impact of the scanner on the workstation when it is running, 155 COM and EXE files totalling 4,965,744 bytes were copied from one directory to another, and the process timed. The directories used for the source and target were excluded from the virus scan to avoid the risk of a file being scanned while waiting to be copied.

The default setting of Best Foreground Application Response Time was used for consistency. Due to the different processes which occur within the server, time tests were run ten times for each setting and an average taken. The four tests were:

- Program not loaded – this establishes the baseline time for copying the files on the server
- Program loaded with Auto-Protect inactive, and the immediate scanner not running – tests the impact of the application in a quiescent state
- Program loaded with Auto-Protect active, but the immediate scanner not running – tests the impact of the on-access component on its own
- Program loaded with Auto-Protect active and an immediate scan running – this measures the full impact of the system

See the summary table for the results. The overhead when running the Auto-Protect or the scanner is significant, but this has to be balanced with the fact that it is checking for compressed files and appears to be doing a very thorough job of the scan. The scan on the test suite viruses took nearly an hour to complete, but produced a good result. [*Norton has recently introduced an emulator into the product, which accounts for both the improvement in detection and the reduction in speed of the scanner. Ed.*]

Summary

Although the installation is very straightforward, there is no mention at all of what to do in the User's Guide. This puzzled me initially, but it transpired that there is information about this in the shipping product.

As for documentation, having an on-line document as well as hard copy is a very useful facility. The on-line help, in addition, provides good support to the user.

The range of options are comprehensive – except for the scheduler. I find it odd that such a limited facility is available within the application, forcing the user to use the system scheduler for any higher level of functionality. I hope this is an interim state of affairs. The software appears to be mainly targeted as a workstation product. The server communication seems to be limited to alerts being sent to the *Norton AntiVirus* NLM, if this is present on the network.

The licence transfer of previous versions to charitable organisations is something of an innovation. It will be interesting to see who takes this up, both in terms of users and other software companies.

To conclude, the problems with polymorphic detection rates in previous reviews have been addressed with a vengeance, moving the score from just under a 60% success rate to the current 100%. Overall, *NAVNT* looks to be a good product with the quality we have come to expect from this developer.

Norton AntiVirus for NT

Detection Results

Test-set[1]	Viruses Detected	Score
In the Wild	341/342	99.7%
Standard	420/511	82.2%
Polymorphic	10000/10000	100.0%

Overhead of On-access Scanning on NT:

Tests show time taken to copy 155 COM and EXE files (4.9MB). Each is performed ten times, and an average is taken.

	Time	Overhead
Program not loaded	7.1	-
Program loaded; no manual scan AutoProtect off	7.3	3.6%
Program loaded; no manual scan AutoProtect on	10.2	44.3%
Program loaded; manual scan AutoProtect on	12.6	78.0%

Technical Details

Product: *Norton AntiVirus for NT v2.0*.

Developer/Vendor: *Symantec Corp*, 2500 Broadway, Suite 200, Santa Monica, CA 90404-3063 USA. Tel +1 310 449 4257, fax +1 310 453 0636, WWW http://www.symantec.com/.

Distributor UK: *Symantec Northern Europe*, Sygnus Court, Maidenhead, Berkshire, UK SL6 8AD. Tel +44 1628 592222, fax +44 1628 592393.

Price: Workstation or server, £69 + VAT. 10-pack, £429 + VAT (10-node licence). Site licence prices from local resellers. Updates included: at least monthly; additionally as required.

Hardware Used:
Server: *Compaq Prolinea 590* with 16MB RAM and 2GB of hard disk, running *Windows NT v3.51*.

[1]**Test-sets:** In the Wild File, In the Wild Boot Sector, and Polymorphic – see *VB*, October 1996, p.17. Standard – see *VB*, November 1996, p.23.

PRODUCT REVIEW 2

Virus ALERT

Dr Keith Jackson

Virus ALERT is a multi-faceted package containing a scanner, memory-resident anti-virus programs, disinfection features, and a disk recovery program. This is not an exhaustive list, and in this review I will only have space to look at the main components. I last reviewed this product for *VB* in June 1995.

The product was provided for review on four 1.44MB floppy disks. Two were marked 'Virus ALERT', one was for macro viruses, and the final disk was marked 'TESTER'.

Documentation

The minimal documentation theme of recent reviews continues – apart from glossy bumph, *Virus ALERT's* printed documentation comprises a single A4 sheet of paper, folded twice to make a little booklet called a 'Quick Reference Handbook'. A single folded sheet of printed documentation was all that was provided for the previous review.

Last time around, the on-line help was criticised for being very skimpy. This version has plenty of on-line help: on-line text files are voluminous, and provide excellent advice for program execution, scanning, backups (e.g. 'Rule #1 is: MAKE BACKUPS!!!'), virus removal and recovery.

One of the documentation files states that viruses cannot spread between different types of computer. This is no longer true. The rise of macro viruses has meant that viruses can now move between any system offering a version of the 'host' program 'compatible' with the macro virus concerned.

Installation

Virus ALERT can be installed for *Windows 95*, *3.1* or DOS. I chose *Windows 3.1*. Starting off involved running SETUP and answering the obligatory question about where installed files should be stored. To confuse matters, a program called SETUP1.EXE was also present on the installation disk.

Things did not run quite as smoothly as the above description indicates. The installation program is not very intelligent about defining a valid subdirectory name. For instance, the name D:\VIRALERT\VIRALERT is rejected as an invalid path. When I tried again with D:\VIRALERT the program appeared to be happy, and all continued.

Things came to a halt when the installation program insisted it could not find a file called A:ALERT.EXE, though it was present on the floppy disk in drive A. The only cure I could find was to start again and specify D:\ALERT as the subdirectory for the product's files – the same name as the usual *Virus ALERT* default, but on a different drive.

Installation then completed: the TESTER diskette was requested, icons for five *Virus ALERT* executable files were created, the changes to AUTOEXEC.BAT were described, and instructions were given on making a Recovery Disk.

When my PC was rebooted, the *Virus ALERT* programs ONGUARD and VASCAN (called by VAGUARD) were visible during the boot sequence, but after VAGUARD had executed, the reboot stopped. The screen was blank! I tried pressing a key (any key) and the message 'MISSING ENDTEXT' appeared. The reboot then continued. Looking into my previous review of the product, the same message appeared whenever installation ended, and every time the scanner completed execution. I didn't know why this happened then, and I still don't. It does, however, need fixing. Still.

Subdirectories and Macros

After *Virus ALERT's* installation program had run its course, I found that eight (yes, eight!) extra subdirectories had been created in the root directory of drive C. These were TESTER, GOOD, SAFETEST, SAFEKEEP, BAD, PASSWORD, NOT-RUN and UTILITY. All were initially empty, except for TESTER which contained 1.08MB in 45 files. I've railed in the past about programs which clutter up my root subdirectory with installed files – this tops the lot. If the product needs this space, it should keep everything in its own subdirectory. The purpose of these subdirectories will become clearer in the description of TESTER (see below).

I tried to install the *Virus ALERT* facilities provided on the MACROS diskette. The installation program seemed to be progressing satisfactorily; displaying reams of guff about the Licence Agreement, bargraphs showing progress (a graphical *tour de force*)… then, a message appeared saying the file WINWORD.EXE could not be found. In short, the MACROS facilities will not install unless *MS Word* is present, which seems fairly reasonable.

Scanning

Executing the main scanner (VASCAN) through the menu front-end program (ALERT) is a bit unconventional. VASCAN is command-line driven, and requires run-time switches to be specified to tailor its execution. A sample command line is provided onscreen, which the user edits to obtain the desired execution of VASCAN. A specific drive is scanned by default, and the results written to a log file and displayed onscreen.

Unfortunately, the space provided onscreen for entering the desired command-line switches is not large – if the line is too long, switches at the right-hand end are ignored. Nothing warns the user of this. Worse, it is not possible to specify multiple command-line switches together to save space. I resorted to having a log file name just one character long so space remained for command-line switches. Less than ideal.

Something curious is going on when VASCAN is executed. Two programs with the same name but different extensions (VALIC.COM and VALIC.EXE), and another executable program, VALICT.COM, are installed. VALIC.COM and VALICT.COM are byte for byte identical. The *Virus ALERT* documentation states (correctly) that only VALIC.EXE is needed for VASCAN to execute. So why the other programs?

Scanning Speed

In its default state, and under *Windows*, VASCAN scanned the hard disk of my test PC in 1 minute 21 seconds (1627 files, 476 files). When VASCAN was executed under DOS alone, this time dropped to 1 minute 15 seconds. By default, files with extensions COM, EXE, SYS, OV?, BIN, DLL, BAT and DO? are scanned. When other VASCAN options are activated, scan times escalate. If every extension is scanned, it rises to 2 minutes 49 seconds. Finally, if all parts of all files are scanned, it increases to 6 minutes 22 seconds.

To reinforce that these scan times are reasonable, I compared *Virus ALERT's* scanning times with two other products. *Dr Solomon's AVTK* scanned the hard disk of my test PC in 1 minute 9 seconds; *Sophos' SWEEP*, in 2 minutes 9 seconds. Scanning all types of files took the *AVTK* 2 minutes 36 seconds. Neither of these programs are slowcoaches: *Virus ALERT's* scanner does indeed execute at a decent pace.

Virus List

VASCAN provides a list of all viruses of which it currently has knowledge. This can be presented onscreen or written to a file (which can be several hundred kilobytes long).

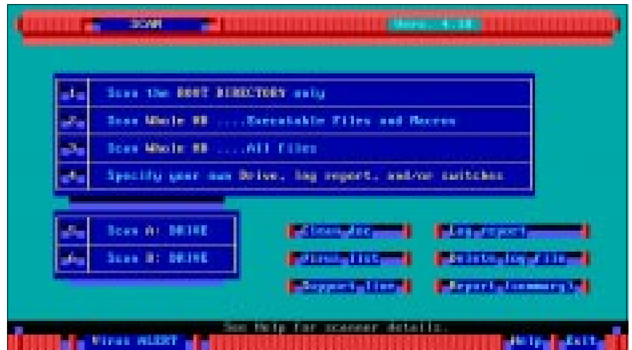
The version of *Virus ALERT* provided for review (signature file dated 25 July 1996) claims to detect 6702 viruses. This breaks down into 6240 file-infecting viruses, 3870 memory-resident viruses, and 587 boot sector viruses. Several viruses come under more than one heading; thus the total number known is less than the sum total of the three figures.

Documentation files state that ONGUARD, the memory-resident file scanner, uses the same virus database as VASCAN, but for some reason ONGUARD only claimed to know about 6568 viruses. I am not certain why this discrepancy exists – see below for more discussion of ONGUARD.

Virus Detection and Macro Viruses

VASCAN can spot packed or compressed files (e.g. LZEXE, PKLITE). By default it does not scan inside such files, but scanning inside compressed files can be activated if desired.

I tested the detection capability against the test-set described in the Technical Details. Against the viruses in the In the Wild test-set, using default settings, VASCAN detected all 286 samples. Similarly, against the viruses in the 'Standard' test-set, again using the default settings, it again detected all samples. Finally, against the polymorphic samples, VASCAN detected all 5500 test samples, again 100%. Additionally, all twenty boot sector samples were detected as infected.



Virus ALERT offers a plethora of options to protect your PC.

When VASCAN's command-line options were activated to scan all parts of all files, the results were unsurprisingly the same as those quoted above.

The product includes a diskette for dealing with macro viruses. Under Installation, I described how this would not install if *Word* was not present – but if detection of macro viruses is a priority over removal, this is not very important. VASCAN itself found all 29 macro virus-infected samples.

False Positives

VB has created a shiny new CD-ROM with over 600MB of executable files (5500 COM/EXE files), which can be used to test products for 'false positives'. *VB* has taken great care to ensure that no file on this CD-ROM is virus-infected.

When *Virus ALERT* scanned this CD it found two infected files. A file called WPROTECT.EXE was falsely thought to have Spanish_Telecom_1, and VIRBOOT.EXE was claimed to be infected with the Brunswick virus. [*Both files are parts of old anti-virus products; however, it is not unreasonable to expect a modern product to deal correctly with them. Ed.*]

Memory-resident Software

Virus ALERT includes ONGUARD and VABLOCK, two memory-resident programs, and a program (VAGUARD) which uses VASCAN to perform a quick check on memory and the important parts of the hard disk. VAGUARD does not become memory-resident. It is intended to be used during a PC reboot. The documentation states that VAGUARD 'has a stellar accuracy for detecting both known and unknown polymorphic and encrypted viruses'.

The memory-resident programs are explained below. They are intended for use within AUTOEXEC.BAT, but like VAGUARD can, if necessary, be executed from the command line as individual DOS programs.

Memory-resident File Detection

ONGUARD is a memory-resident program which inspects executable files before they are executed. The developers of *Virus ALERT* have been very open, stating clearly that file content is only scanned at the time of program execution, not whenever the file is accessed. Therefore, infected programs can be copied but they are prevented from being executed (if ONGUARD successfully detects the virus). With an honesty rare amongst anti-virus developers, the on-line help states that this 'feature' was introduced to prevent ONGUARD imposing a large overhead on program execution. Most products that I review skirt around this problem.

I measured the overhead imposed by ONGUARD by copying the product's files (52 files, 1.33MB) from one subdirectory to another. Normal copying time was 13.7 seconds, increasing to 14.5 seconds with ONGUARD present. Why the overhead is anything other than infinitesimal when ONGUARD is not checking files during copying is not explained.

Behaviour Blocking

VABLOCK is (unsurprisingly) a program which 'blocks any suspicious activity and therefore is effective against unknown viruses'. In short, a behaviour blocker. A precise definition of 'suspicious' is not provided. By default, COM, EXE, SYS, BIN, and SIG files are monitored. I'm not sure how best to review VABLOCK. It does not claim to be a panacea; the relevant documentation file states that if a virus bypasses the OS and attacks the hardware directly, nothing will be detected. Some (though not all) interrupts are monitored by VABLOCK.

In common with all other behaviour blockers I have reviewed, VABLOCK is too intrusive, and when it does pop up it asks questions most users cannot answer. For example, *Norton Commander* maintains its status as a BIN file: whenever I used this program a 'RED ALERT' message box appeared onscreen. Even though I selected the menu option to permit this action, the message box still appeared. Every time.

Tester

A diskette called TESTER was installed as part of the *Virus ALERT* package. TESTER scans the contents of an archived file (by using VASCAN with other tests). This can be useful for testing production software before its final release. It moves any archive file being checked into the \SAFETEST directory, then de-archives it, to scan it for viruses. When the tests are complete, the tested files are sorted into the following separate subdirectories: \GOOD – OK, \BAD – a VIRUS was detected, \PASSWORD – needs a PASSWORD to unpack, \NOT-RUN – memory or unpacking error.

The idea is laudable. It may do what it claims. However, it did nothing on my PC. Executing TESTER under DOS or *Windows*, I placed some archive files to be tested into C:\SAFEKEEP, loaded utilities in C:\UTILITY, and bashed on. There was lots of onscreen activity, VASCAN executed (twice), and files were copied into SAFETEST, but no tested files appeared.

TESTER is responsible for the multiplicity of subdirectories *Virus ALERT* requires, but all these contained nothing. This failure to do anything may have something to do with the fact that installation into anything other than C:\ALERT was problematic (see above); however, something called TESTER should be tested a smidgin better than it has been.

The Rest

In common with some scanners, *Virus ALERT* does not provide the ability to disinfect viruses from infected files, only from infected boot sectors. The software replaces the boot sector of the infected disk with a new clean one (in the case of floppies), or with a previously-saved backup (hard disks). The help provided for disinfection is thorough, and even recommends the immediate remake of a Recovery Disk once disinfection of a virus is complete.

I've run out of space in this review, but also included are VIEWER (makes *Virus ALERT's* log files available onscreen for inspection), LOOK (inspects/edits a file), and RECOVERY & RESTORE (makes/restores machine-specific details stored on diskette). Several other executable programs installed by *Virus ALERT* seem to do nothing – I suppose they are called in some way by the programs which interact with the user.

Conclusions

What do I like about this product? Simply that the results quoted above mean 100% correct virus detection. *Virus ALERT* was capable of detecting every single virus-infected file I threw at it. What more can one ask? Brilliant.

What don't I like? The multiple subdirectories the product insists on installing in the root directory of my hard disk. I cannot see the point – more software development would surely be worthwhile to prevent the spread of this detritus.

In summary, *Virus ALERT* contains a scanner which is quite quick, and is currently perfect at detecting viruses. What can be expected of the next version? Watch this space…

Technical Details

Product: *Virus ALERT v4.10-09*; serial number 0000037.

Developer/Vendor: *Look Software Systems Inc*, 4659 Albion Rd, Ottawa, Ontario, Canada K1X 1A4. Tel +1 613 822 2250, fax +1 613 822 2160, BBS +1 613 822 2159, email sales@look.achilles.net.

Availability: At least 450KB of RAM to execute scanner. The menu system adds another 50KB. ONGUARD requires 8KB; VABLOCK, just over 10KB.

Price: Single-user licence – US$69.95
Corporate licences: 5-pack – US$199.95
10-pack – US$299.95
25-pack – US$398.75
Price on application for site licences starting at 50 users. Includes updates as released.

Hardware used: A 33MHz 486 clone, with 12MB of RAM, one 3.5-inch (1.44MB) diskette drive, one 5.25-inch (1.2MB) diskette drive, 1GB of hard disk space, running under *MS-DOS* v5.0 and *Windows v3.1*.

Viruses used for testing purposes:

Where more than one variant of a virus is available, the number of examples of each virus is shown in brackets after the virus name (if the total is greater than one). For a complete explanation of each virus, and the nomenclature used, please refer to the list of PC viruses published regularly in *VB*. A listing of the boot sector viruses can be found in *VB*, March 1996, p.23. Listings for the other test-sets are in *VB*, January 1996, p.20.

SUBSCRIPTION RATES

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

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

Editorial enquiries, subscription enquiries, orders and payments:

Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, England

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

US subscriptions only:

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

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

END NOTES AND NEWS

***Sophos Plc's* next rounds of anti-virus workshops** will be on 29/30 January and 19/20 March 1997 at the training suite in Abingdon, UK. Additionally, the company's training team is hosting a Practical NetWare Security course on 21 January and 13 March 1997 (cost £325 + VAT). The company has also released the latest version of its disk authorisation software, *D-FENCE*, which includes high security disk encryption. Information on courses and products 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/).

SecureNet Technologies has announced the latest release of its flagship product, *V-NET*, in the USA. Available in the UK under the name *Enforcer* from *Precise Publishing*, **this anti-virus software package automates the protection process**. As *VB* went to print, the product was unavailable for review. Information from *SecureNet* in the US on Tel +1 206 776 2524, or from *Precise Publishing* in the UK; Tel +44 1384 560527.

The proceedings of the sixth *VB* conference are available; price £50 + p&p. To order, contact conference coordinator Alie Hothersall; Tel +44 1235 544034, email alie@virusbtn.com.

McAfee Associates has launched a 'Christmas promotion' for its *VirusScan*: **a five-in-one multi-platform CD, available until the end of January 1997**, which includes a free copy of *McAfee's QuickBackup for Windows 95 and Windows NT*. The pack is expected to retail at £49.99. For further information, contact Caroline Kuipers on Tel +44 1344 304730, or email caroline_kuipers@cc.mcafee.com.

Dr Solomon's Software (formerly *S&S International*) is presenting **Live Virus Workshops** at the *Hilton National* in Milton Keynes, Bucks, UK on 19–20 February 1997. Details from the company: Tel +44 1296 318700, Web site http://www.drsolomon.com/.

InfoSecurity 1997 will take place at Olympia 2 (London, England) from 29 April–1 May 1997. The event is planned to address all aspects of IT security in the business environment, and many anti-virus developers will be present. For further information, contact Yvonne Eskenzi on Tel +44 181 449 8292.

Command Software Systems has announced the release of its new anti-virus SMTP email gateway. The company states that the combination of its anti-virus product, *F-PROT Professional*, with 'state of the art' email gateway technology will provide **protection against the threat of viruses transmitted via the Internet.** Information on this and other *Command* products can be found on the company Web site; http://www.commandcom.com/.

Reflex Magnetics will be hosting another round of **computer security courses in the New Year**: Managing Data Protection (7 January 1997), UNIX Threats and Vulnerabilities (4 February 1997), Internet Security and Firewalls (5 February 1997), Live Virus Experience (19–20 February 1997) and The Hacking Threat (4–6 March 1997) will all take place at *Reflex's* premises in London, England. For further information, contact Phillip Benge at *Reflex Magnetics*; Tel +44 171 372 6666.

OPSEC (***Open Platform for Secure Enterprise Connectivity***), a single platform which integrates and manages all aspects of network security, has been released by *CheckPoint Software Technologies.* The product provides built-in applications for, among others, access control and authentication. For further information, contact the company on Tel +44 1123 421338, or visit the Web site; http://www.checkpoint.com/.

British-based *Highwater Signum Ltd* has announced the development of an **indelible electronic 'fingerprint'** which permanently records the name of the owner/creator of an image. Further information from Alan Bartlett; Tel +44 1242 221390, email alanb@hwuk.demon.co.uk.