ISSN 0956-9979 JANUARY 1998

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

IN THIS ISSUE:

• **Glazed and confused?** This month's comparative review looks at twenty *Windows 95* anti-virus products. Who attained the first VB 100% ItW awards? See for yourself, starting on p.10.

• **Welcome guest:** *Virus Bulletin's* Technical Editor takes the chair and tells it like it is. Read what Jakub Kaminski has to say in his guest editorial on p.2.

• **Out to get you:** Our virus analyses this month feature a neurotic pair. DarkParanoid and Win 95.Anxiety get the full treatment, starting on p.7.

CONTENTS

EDITORIAL

I say Virus, You say Trojan

The basis of any successful information exchange is the common understanding of the language used by all parties involved. As long as we all know that while 'I say tomato, you say tomato', we are still talking about the same thing, and we can have a fruitful discussion. However, if you mention bananas and I start discussing 'ananas' ('pineapple' in many European languages), we will soon be in deep trouble. If we don't figure out quickly that we are talking about different things, our dialogue will become the source of confusion and doubts in each other's mental abilities.

"how do we classify the code to define its nature?"

Most new technology, especially in computer and programming terms, reflects the considerable effort of rendering new inventions and discoveries more comprehensible by naming them after existing, well-known objects or subjects with analogical features/behaviour. While some analogies are obvious (few cannot yet distinguish a hard disk from a floppy), most terms, recognizable in inner circles, are meaningless to outsiders. For those not involved in Electronics, a 'floating gate' might have more in common with a sluice than a computer.

The biological analogy of the term 'virus' reflects similarities in the behaviour of computer and biological viruses perfectly. It also acts as an intuitive aid to understanding the nature of computer viruses. The term 'trojan' is commonly used by the anti-virus and computer security industries to specify a certain type of malicious software. To 'outsiders' though, it would sound more like a contraceptive product and, to historians in particular, it is likely to conjure up visions of the wooden horse the Greeks built while besieging Troy (from which the analogy derives). The idea of 'a worm' crawling through one's machine usually beats the imagination of an average PC user.

The anti-virus industry has been doing its best to increase awareness of virus threats. In a way, it has been successful – now, if anything goes wrong, the first thing people look for is a virus. Virus detection and removal is perceived by some users as a very clever, almost magical process, but there is no reason a magician shouldn't do easy tricks as well as difficult ones. If you are a 'good guy', tracking and fighting thousands of viruses, why don't you fix some silly, non-replicating trojans, worms, jokes and corrupted files? If trojans seem to be more dangerous than viruses, why don't anti-virus vendors tackle those too?

Because they argue that, by definition, they develop anti-virus, not anti-trojan or anti-malware, software. Some try to meet demand by including in their products the detection of trojans and jokes. At this stage, users should be able to have a clear picture of who's detecting what. Of course, this is assuming that everyone involved in anti-virus research knows how to classify code and agrees on what a virus is, what a trojan is… etc. Unfortunately (or not,) complexity is the essence of the universe; the world (including that of viruses) is not black and white with borders clearly and forever defined. The more we know about viruses and other malicious software and the greater the diversity of ideas and tricks implemented, the more valid are the arguments for new classification and naming schemes. There is a strong desire to do things right and not to compromise one's principles – this is often the position of anti-virus researchers. Sometimes, however, adhering to these priciples makes it difficult to provide the clear answers and simple solutions that users prefer.

The latest and one of the longest such discussions (two months to date) has centred on the classification of so-called AOL trojans. There are more than enough reasons to categorize at least some of them as viruses, but at the same time, there are legitimate arguments to classify them as trojans or even worms (based on respective definitions). All agree, however, that it is unwise to misname these programs for the convenience of either the anti-virus community or users, but how do we classify the code to define its nature? The worst possible outcome is to assign the multiple label 'trojan virus' or 'virus trojan'. This is not only confusing, but contrary to current standards. Whatever the outcome, this will always be a controversial entry in the anti-virus dictionary. This is not the first and certainly will not be the last case of its kind.

Jakub Kaminski, Technical Editor

VIRUS BULLETIN **©1998 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /98/$0.00+2.50**

NEWS

Going Global

On 1 January 1998, the *National Computer Security Association* (*NCSA*) became the *International Computer Security Association* or *ICSA*. The company says the name change reflects its increasing international presence and its efforts to improve computer security on a global scale.

Last year, nearly a third of the *NCSA's* consortia, professional members, partners, research, conferences and other activities were centered in Europe or Asia. In the first quarter of 1998, the *ICSA* plans to expand its influence in those continents by introducing satellite companies in Amsterdam and Tokyo ▮

mIRCy Dealings

In mid-December 1997, the anti-virus world was briefly awash with talk of yet another new form of virus. The most popular *Windows* IRC (Internet Relay Chat) client software, known as *mIRC* (pronounced 'murk') was configured by default to use the same directory for its download and script files. Add to this the fact that a file in the script directory called SCRIPT.INI is automatically run if it exists, and most readers can probably see a problem that the *mIRC* authors missed in their initial design.

As extensive file transfer is common on IRC, unsuspecting users accepting copies of SCRIPT.INI opened themselves to a range of IRC indignities. Fortunately, none of the widely distributed scripts taking advantage of this security hole (or 'feature', as you will) performed any serious damage. It must be noted that the *mIRC* developers, who were aware of increasing exploitation of this hole about a month earlier, had an upgrade almost ready to distribute as interest in the problem peaked. All *mIRC* users should upgrade to version 5.3 or above and familiarize themselves with the risks.

All IRC users should check that their client is not configured in a similarly dangerous manner and should check what (if any) the default script name for their client software is. Refusing to accept downloads in that name is generally a good idea. Security-conscious IRCers should turn off automatic acceptance of downloads (DCC autoget). A good explanation of the *mIRC* problem and several other general IRC security concerns is available on the Web at http://www.irchelp.org/ ▮

Another Hoax – Yahoo!

The ever-popular www.yahoo.com was not infected with a computer-melting super-virus, set to trigger on 1 January 1998. News reports to this effect in December have clearly been proven wrong. There is good coverage of the story at http://www.wired.com/news/news/technology/story/9059.html ▮

Prevalence Table – November 1997

Virus	Type	Incidents	Reports
CAP	Macro	126	23.1%
Concept	Macro	38	7.0%
Npad	Macro	30	5.5%
AntiEXE	Boot	27	5.0%
Form	Boot	25	4.6%
Laroux	Macro	21	3.9%
AntiCMOS	Boot	19	3.5%
Empire.Monkey	Boot	18	3.3%
Parity.B	Boot	18	3.3%
Wazzu	Macro	16	2.9%
Dodgy	Boot	14	2.6%
Ripper	Boot	13	2.4%
NYB	Boot	12	2.2%
Junkie	Multipartite	10	1.8%
Maverick.2048	File	10	1.8%
WelcomB	Boot	9	1.7%
Imposter	Macro	8	1.5%
One_Half	Multipartite	8	1.5%
Appder	Macro	7	1.3%
Feint	Boot	7	1.3%
Parity.A	Boot	6	1.1%
ShowOff	Macro	6	1.1%
Temple	Macro	6	1.1%
EXEbug	Multipartite	5	0.9%
Spanska.4250	File	5	0.9%
Kompu	Macro	4	0.7%
MDMA	Macro	4	0.7%
Edwin	Boot	3	0.6%
INT40	Boot	3	0.6%
Muck	Macro	3	0.6%
NiceDay	Macro	3	0.6%
Stoned.Angelina	Boot	3	0.6%
V-Sign	Boot	3	0.6%
Others [1]		55	10.1%
Total		545	100%

[1] The Prevalence Table includes two reports each of: Baboon, Demon, Die_Hard.4000, Gable, Galicia.800, LBB_Stealth, Pieck, Sampo, Simple, Stoned and Tequila; and a single report of each of: Barrotes, Burglar.1047, Cascade.1661, Cascade.1701, CountTen, Cruel, DamnFog.1748, DarkAvenger, DelCMOS, DZT, Fairz.2340, Finnish_Sprayer, Green_Caterpillar, IVP.2385, Johnny, Jumper.B, Maverick.1536, NF, NOP, Phalcon.1168, Quandary, Rehenes, RP, Russian_Flag, Schuman, Shell.10634, Stealth_Boot, Swiss_Boot, Swlabs, Trivial.71, Unashamed, Urkel and Werewolf.1208.

IBM PC VIRUSES (UPDATE)

The following is a list of updates and amendments to the *Virus Bulletin Table of Known IBM PC Viruses* as of 15 December 1997. Each entry consists of the virus name, its aliases (if any) and the virus type. This is followed by a short description (if available) and a 24-byte hexadecimal search pattern to detect the presence of the virus with a disk utility or a dedicated scanner which contains a user-updatable pattern library.

Type Codes

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

Androide.985

CER: An encrypted, appending, 985-byte virus containing the text 'Androide 1a by WM [DAN]'.

```
Androide.985        2E8A 9E14 01BF AF03 8BCF 8DB6 2D01 2E30 1C46 B42E CD21 E0F6
```

Bachkhoa.3544

CER: An encrypted, appending, 3544-byte virus containing the texts 'CHKILST.MS', 'CHKLIST.CPS', 'FILESIGN.SAV', 'FILE_ID.DIZ', 'Ha Noi University of technology.' and 'Your PC was infected by BACHKHOA virus.'. The payload, which triggers on 25 November, overwrites the contents of the hard disk (starting at the first FAT). Infected files have their time-stamps set to 62 seconds.

```
Bachkhoa.3544       B9BC 03D1 E983 E910 2E31 0783 C302 E2F8 C32E A3D8 0E2E 891E
```

Bazil.1956

CR: An encrypted, appending, 1956-byte virus containing the texts '* THIS FILE IS INFECTED AS WELL AS ALL COM FILES ON THIS DISC! *' and '[BaZiL]'.

```
Bazil.1956          8B3E 0101 81C7 0001 E803 00E9 3902 B93E 05BB 5302 03DF 8037
```

Blurp.4733

CER: An appending, 4733-byte virus containing the texts 'KERNEL32.DLL', 'USER32.DLL', 'GetModuleHandleA', 'GetProcAddress', 'MessageBoxA', 'CreateFileA', 'CreateFileMappingA', 'MapViewOfFile', 'UnmapViewOfFile', 'CloseHandle', 'FindFirstFileA', 'FindNextFileA', 'FindClose', 'LoadLibraryA', 'GetLocalTime', '*.*', '*.COM' and '*.EXE'. Infected files have the word 293Bh (';)') at offset 0003h in COM files and at 0012h in EXEs.

```
Blurp.4733          B829 3ACD 213D 293B 745B 8CC0 488E D833 FF80 3D59 764F 816D
```

Bowl.903

CN: An appending, 903-byte, fast, direct infector containing the texts ').com', '*.zip', '*.arj', 'anti-vir.dat' and '????????COM'. The payload, which triggers on 25 December, tries to overwrite 666 sectors on drive C and displays the string '..... ....', locking the system up.

```
Bowl.903            B440 B987 038D 9603 01CD 212E FE06 7204 EB89 0EE8 4900 B43B
```

Dsoft.434

CR: A prepending, 434-byte virus containing the texts '*.com' and 'DAREKSOFT ss'. The second string is displayed on 14 June.

```
Dsoft.434           BA00 01B4 40B9 B201 CD21 7304 1FEB 1A90 1FB8 0242 31C9 31D2
```

Ebola.6001

EMR: A multi-partite, polymorphic, stealth, appending, 6001-byte virus containing the texts '** Ebola is present **', '## (Copyleft) DD.MM.YY by M² GERMANY ## (V1.1)', 'Eeehhjj, Du genetischer Abfall !!!', 'Na, haben wir denn gerade einen Fehler gemacht ? Vorab möchte ich mich kurz vorstellen: Mein Name ist Ebola, ich wohne auf Deiner FESTplatte, arbeite zur Zeit auf Deinem Rechner, ernähre mich von Deinem Datensalat, habe Angst meine Arbeit und meine Wohnung zu verlieren und ich weiß bescheid. Dummerweise will mich mein Vermieter loswerden, er hat wohl gerade irgend ein 'Schädlingsbekämpfungsmittel' eingesetzt. Ich werde nun wohl besser verschwinden. Ach, übrigens: Viel Spaß bei der Renovierung meiner Wohnung ! the crazy program from MM Und Tschüß, (bis demnächst...) Runtime error 032 at 0040:0074 (A)brechnen, (W)iederholen, (I)gnorieren? TYPE Happy Birthday Markus Thank you very much for the congratulations.' and 'CHKDSK SCANDISK DISKFIX TNTSCAN CPAV MSAV SCAN CLEAN IBMAVD IBMAVDQ IBMAVSP IBMAVSH VWATCH VSAFE VSHIELD VSHLDCRC VSHEML CHKVSHLD '. The virus infects EXE files and the Master Boot Record on hard disks. The virus payload displays the long message, locks the keyboard after making the text fade away, corrupts CMOS settings and reboots the system. Infected files cannot be reliably detected using a simple template, however the following pattern can be used to detect the virus in memory and MBRs.

```
Ebola.6001          FA33 DB8E D3BC 007C FB36 832E 1304 0790 CD12 B106 D3E0 8EC0
```

Gee_zee.464

ER: An appending, 464-byte virus containing the text 'Gee_Zee 2'. Infected files have the word 0300h at offset 0010h (SP) and the word 01AFh at offset 0014h (IP). The payload sets the video mode to 3 and hangs the system.

```
Gee_zee.464         EFCD 2180 FCF0 74D2 B853 008E C0B9 D001 FCF3 A4EA 5A01 5300
```

Jorgito.543

ER: An appending, 543-byte virus. Starting from January 1998, the virus displays the encrypted message 'Jorgitø Was Here'.

```
Jorgito.543          BBD7 F993 CD21 3D83 7874 55B8 2135 CD21 2E89 1EF6 012E 8C06
```

MystiqueLeech.1017

EN: An encrypted, appending, 1017-byte direct infector infecting two files at a time. The virus contains the plain-text string 'Mystique Leech 10/97 (c) m-A-X!' and the encrypted message '****************************** * The Mystique Leech! * ****************************** * Hi Software Pirate * * Leeching gamez and appz * * from IRC is not good * * for your computer and * * s o f t w a r e! * * Have fun hunting this one * * and stay away from IRC! * ******************************'.

```
MystiqueLeech.1017  9090 BAD8 0190 902E 812F ???? 438B CA8B D143 8BCA 8BD1 4A75
```

Npox.1602

CER: A stealth, appending, 1602-byte virus containing the text 'This is a production of the Highworth Warneford School Corrupt Programers. Tel 666 for a cure. [HWS-CP v1.0]'. Infected files have the word DBDBh at the end of their code.

```
Npox.1602            BA03 01B9 4206 B440 E89F 0272 F02B C875 EC8B D1B8 0042 E891
```

PS-MPC.646

CER: An encrypted, appending, 646-byte virus containing the text '[Oh! Happy! Happy! Joy! Joy!] [These files are fucked Stimpy!] Doobage King [Ren & Stimpy Virus]'. Infected .EXE files have the word 475Ah ('ZG') at offset 0010h.

```
PS-MPC.646           BB?? ??B9 3B01 2E81 37?? ??43 43E2 F7??
```

PS-MPC.1427

CR: An appending, 1427-byte virus containing the texts 'PARANOID [VD/SLAM]', 'Wrong choice sucker! hehehe... ;-)' and 'Central Point Anti-Virus (c) 1993 CPS Self Integrity Check warning - File was changed ! Choose an option: [R] Self Reconstruction. [C] Continue execution. [E] Exit to DOS. Press R,C or E:'.

```
PS-MPC.1427          A39E 05B4 40BA 0000 B993 05CD 21B8 0042 33C9 999C 2EFF 1EDF
```

Sailor.1107

CER: A minor variant of the Sailor.1108 virus containing the same texts 'Sailor.Mars', '-b0z0/iKx-' and 'OCANIFVITICSIV-FVABT'. Infected files have their time-stamps set to 28 seconds. The virus can be detected using the same template (see *VB* July 1997, p.5).

SillyC.159

CN: An appending, 159-byte, direct infector containing the text '*.com'. Infected files have the byte 7Bh ('{') at the offset 0003h.

```
SillyC.159           2D03 0089 8696 00B4 40B9 9F00 908B D5CD 21B8 0042 33C9 99CD
```

Supervisor.1448

CR: An appending, 1448-byte virus containing the texts 'SERVER', 'SECURITY_EQUALS', 'PASSWORD' and 'SUPERVISOR'. Infected files have the string 'MsDos' at the end of the code.

```
Supervisor.1448      9C2E FF1E 1200 B440 B9A8 0590 0E1F 2E8B 1E4B 00BA 0000 9C2E
```

Tarazona.985

CR: A stealth, multiple encrypted, appending, 985-byte virus containing the texts 'Tranquilo chico que si no es en septiembre será en Junio :-)', 'Que los 12 créditos mínimos te acompañen', 'by nEUrOtIc cPu cOrpOrAtIOn S.A.' and 'Virus Tarazona_Killer por NigromanteZ'. Infected files have their time-stamps set to 60 seconds.

```
Tarazona.985         4749 75F6 B983 0333 FF3E 8A86 D004 3E30 834D 0147 4975 F7C1
```

TPVO.1575

CER: An appending, 1575-byte virus containing the texts 'COMMAND IBM PC TB CKVI KLVI DEVI BTOOL RTOOL TDISK SCAN CLEAN' and 'Your PC was now OPEN! Whao! Ha! Ha! Ha! Ha! == Written by Zhuge Jin at TPVO , 1995 == === Taiwan Power Virus Organization. ==='.

```
TPVO.1575            72A0 2689 4515 B440 B927 0633 D2E8 9000 E8FC 00EB 8D83 7C1A
```

Trivial.40.J

CN: An overwriting, 40-byte virus containing the text '*.com'.

```
Trivial.40.J         023D BA9E 00CD 2193 B440 BA00 01B9 2800 CD21 B43E CD21 CD20
```

Typebug.951

CR: An encrypted, appending, 951-byte virus containing the texts 'The TRUTH is out there...', '-=> Typebug v1.02 <=- by Zymotic/[HVM] - Hungarian Virus Academy.' and 'HVM have three members: Zymotic, MindStorm and Wyvern.'. The virus intercepts Int 16h (keyboard services) and plays tricks with entered keystrokes.

```
Typebug.951          4374 09C7 06?? ???? ??E9 0000 BE?? ??B9 9F03 8034 ??46 E2FA
```

Ugur

CER: Two appending, 1297-byte and 1320-byte variants of the Ugur family. The viruses contain the text 'UGUR MUMCU öLMEDi..'. Infected files have their attributes set to Read Only. The payload overwrites the first 200 sectors on drive C.

```
Ugur.1297            B911 05B4 40E8 E401 33C9 33D2 B800 42E8 DA01 BAA3 04B9 0300
Ugur.1320            B928 0590 B440 E8EF 0133 C933 D2B8 0042 E8E5 01BA BA04 90B9
```

V.181

CN: An appending, 181-byte, fast, direct infector containing the text '*.com'. The virus reinfects already infected files.

```
V.181                B440 B9B5 008D 9600 01CD 218B 8601 012D 0300 8986 B301 B800
```

Waca.1700

CER: An appending, 1700-byte virus containing the encrypted texts 'Satana brings you much pain! You forgot that !', 'COMMAND.COMCOMEXEDOCHLPPASARJBACKUP.COM' and 'If you want to die DO IT IN MIDNIGHT! [acaW]'.

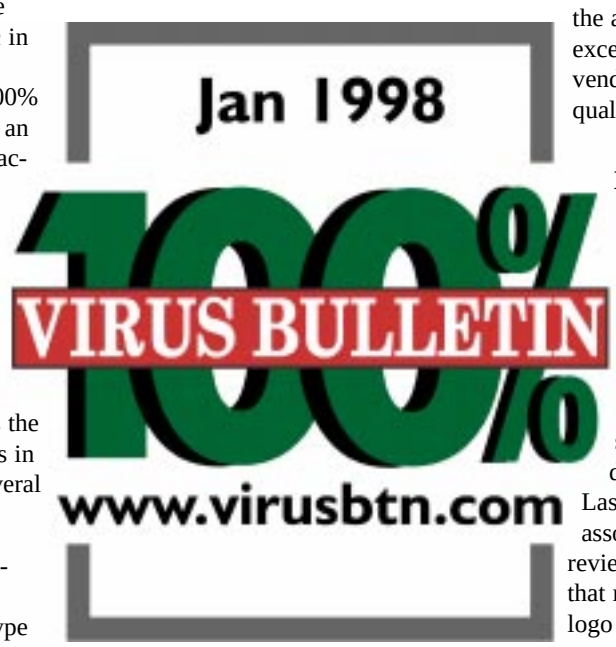
```
Waca.1700            8ED0 E882 04B4 BDCD 21FA 80FC FF75 03E9 A600 BF00 01B9 A406
```

FEATURE

VB 100% Awards

This issue sees the inaugural VB 100% awards presented to the products that attained 100% detection against the combined *Virus Bulletin* In the Wild test-set. *Virus Bulletin* anti-virus software tests are the authoritative tests recognized by the anti-virus industry. The VB 100% awards allow us to reciprocate that acknowledgement by giving the vendors a mark of achievement that can be clearly and universally recognized.

The VB 100% logo itself simply expresses the idea that qualifying products detected all In the Wild viruses in *Virus Bulletin* tests. The logo includes the month of the issue of *Virus Bulletin* in which the qualifying results were published. This means that a VB 100% award is not written in stone, but is an on-going concern, requiring manufacturers to keep their products up to date with the latest virus recognition techniques and requirements.



What is it For?

The products given VB 100% awards should be seen by potential purchasers of anti-virus software as the most up-to-date achievers. Often, as in this month's issue, there will be several products to choose from.

In keeping with *Virus Bulletin* tradition, this new feature allows our readers to cut through marketing hype and misleading artwork which has been characteristic of some anti-virus product marketing and packaging.

What Does it Mean?

The attainment of a VB 100% award means that the version of the product tested detected all viruses acknowledged as being 'in the wild' by their inclusion in the WildList that was current at the cut-off date for product submissions for the relevant test. For example, if testing products released in January 1998, we will use the WildList published in January. This is a more stringent test than that applied by some commercial certification companies, whose standard tests typically use a WildList two to three months prior to the product release date.

Also, unlike other certification schemes, VB 100% does not allow re-testing. The WildList is a publicly-available document and for most tests, vendors submitting products to *VB* for review would have at least two weeks between WildList updates and product submission for *VB* testing. Products that do not already detect viruses that are newly added to the WildList show a lag in their research and/or intelligence gathering. Not being able to attain a VB 100% award should be the least of their problems.

As an independent anti-virus software tester, it does not behove *Virus Bulletin* to maintain an advertising clientele, nor to pander to vendors paying for product testing or certification processes. The VB 100% awards are made free of charge to all products meeting the detection requirements described earlier. The small incremental cost of maintaining the awards scheme is met by *Virus Bulletin*, to ensure that the awards can stand as recognition of excellence in performance for the vendors and as a guide to product quality for consumers.

How Can You be Sure?

The terms and conditions for use of the VB 100% logo disallow modification of the artwork. A further condition prohibits associating the VB 100% logo with performance claims, descriptive text, or the like, that suggests the associated product detects '100% of all viruses'. Lastly, the recipient may only associate the logo from a given review with the product pertinent to that review. For example, a VB 100% logo awarded to a *Windows 95* scanner cannot be used in the direct promotion of the vendor's *Windows NT* product.

As the anti-virus world is not yet free of snake-oil traders, you can always check the complete list of *bona fide* recipients of VB 100% awards on the World Wide Web at http://www.virusbtn.com/100/.

Who Has One?

Following the testing for the January 1998 *Windows 95* comparative, VB 100% awards have been earned by *Command F-PROT Professional v3.00*, *Norman ThunderByte Virus Control v8.03*, *Norman Virus Control v4.20* and *Sophos SWEEP v3.01a*.

The next two months will be very busy for the *Virus Bulletin* product testing team. There is a DOS comparative appearing in the February issue, and testing for the March *Windows NT Workstation* comparative is under way.

VIRUS ANALYSIS 1

High Anxiety

Péter Ször
Data Fellows

The *Windows 95* platform is becoming an increasingly obvious and attractive target for virus writers – the number of different ways to implement working *Windows* viruses appears to be virtually endless. The latest variation of this trend is Win95.Anxiety, an unoriginal, slightly modified variant of Win95.Harry. Anxiety fixes a few of Harry's small bugs, which is why it is more successful, but some of the original release's fatal bugs still remain. So far, Anxiety is in the wild in Germany, Finland, Holland and the USA. Thus, it seems reasonable to assume that the source of the original infection is related to some FTP site.

Win95.Anxiety infects PE (Portable Executable) programs under *Windows 95*. Further, it can hook the IFS (Installable File System) without having a VxD dropper tailor-made for this purpose. Viruses such as Punch and Memorial are complex because they solve the problem of file system hooking with a specific VxD dropped by the PE part of the virus code and then have to arrange for the VxD to be loaded somehow. This makes them more complicated to write, although virus writers seem to have been optimizing the technique. Anxiety takes a quite different approach; that of patching its code into the Virtual Machine Manager (VMM) of *Windows 95*.

Executing the Virus

When an infected PE program is executed, Anxiety takes control. Programs are executed at *Windows 95's* application level, so they cannot perform system level functions in the way a VxD can. Anxiety bypasses this inconvenience by installing its code into the VMM, which runs in Ring 0.

Anxiety's installation routine searches for a large hole in the VMM's code area, above the address 0C0001000h. If a large enough area (consisting only of FFh bytes) is detected, the virus looks for the VMM header at 0C000157Fh, and checks the area by comparing it with 'VMM'. It saves the address of the Schedule_VM_Event system function from the VMM for later use, copies its code into the previously-located hole in the VMM, and changes the Schedule_VM_Event address to point to itself. Finally, Anxiety executes the original host program by jumping to its original entry point.

Hooking the IFS

Before the host program can be executed, the VMM will call Schedule_VM_Event, causing the virus' initialization routine to run. As this code is executed in Ring 0, it is able to call VxD functions. Anxiety hooks the IFS by calling IFSMgr_InstallFileSystemApiHook from its initialization code. This installs the new hook API, and after that something peculiar happens.

The code here looks as if it opens and closes a file and calls some registry functions (with invalid parameters!). At first glance it looked like very tricky stuff, until the similarity to Win95.Harry was noticed. Anxiety actually contains some dead code from Harry. One of the areas in which the latter virus is not very successful is its activation routine. Harry creates a cursor image file called C:\SYRINGE.CUR and tries to activate it by modifying the registry. Usually Harry crashes at this point.

It could be that Anxiety was modified to prevent the execution of the risky instructions involved in the above procedure. Anxiety does not have a completely new activation routine, but the modified virus is able to replicate under most *Windows 95* environments without Harry's original problems.

After hooking the IFS, Anxiety resets the address of Schedule_VM_Event to point back to the original, and jumps to Call_VM_Event. The original host will be executed by *Windows 95* a second later.

Infecting PE Programs

Once Anxiety has successfully hooked the file system, it waits for file-open calls. During these, the virus converts the file names with the UniToBCSPath function and checks their extensions. After ensuring the file extension is EXE and that it is in PE format (by looking for the 'PE00' marker), Anxiety opens the file in write mode.

It then reads to the last section header and checks for an existing infection by comparing the seventh byte of the section name with FFh. Usually the last section name is .reloc (followed by a null, 00h). If the program is not considered to be infected, Anxiety patches the section header's other fields to fit into it. The same technique is used by Win32.Cabanas (see *VB*, November 1997, p.10) to make infection less risky and to reduce the chance of detection by heuristic scanners. Then, in a complicated procedure, the virus adds its code to the image.

When VxD code is executed, calls are patched by the VMM. This turns CD20h, <function id> (Int 20h, <function id>) into FAR CALLS. Some of the VxD functions consist only of a single instruction. In those cases, the VMM patches a further six bytes to make the single instruction fit. The VMM does this dynamically with all executed VxDs to speed up their execution. This on-the-fly VxD function

patching means the virus is unable to copy its image immediately to files, since those applications would not work in a different *Windows* environment. Anxiety has a function which patches all its VxD functions back to their normal format, and only then will it save its code into the host program. Various PE header fields are modified to reflect the host's infected state. Finally, the characteristics of the last section are set to MEM_EXECUTE and MEM_WRITE, then Anxiety closes the host program.

The Bug

Unfortunately (from the disinfection point of view), Anxiety has the same problem as Harry. When the virus infects a file, it overwrites part of the original program, usually containing zeroes, because of the section alignment. This makes disinfection difficult and often impossible. Programs ending in code will not work after infection and cannot be repaired by a disinfector. Most of the time, however, the application ends in a long zero-filled area, and the virus works without any noticeable problems, making disinfection possible. The text 'Anxiety.Poppy.95 by VicodinES.' is viewable in the code, but never displayed.

Conclusion

The number of different techniques used by virus writers is growing as quickly in the *Windows* environment as it did in the early days of DOS viruses. The most successful infection methods (introduced by the 'pioneers') will eventually become the 'standard' infection techniques of the next century. Although this 'standard' is not ready yet, it will be finalized during the next few years. As *Windows* virus writers share source code with each other, buggy viruses can currently be fixed by any of those who introduced them into the wild.

Win95.Anxiety

Aliases: Win95.Harry.B.

Type: *Windows 95* PE infector.

Self-recognition in Files:
FFh at offset 7 in the last section header's name area.

Self-recognition in Memory:
Not needed.

Hex Pattern in PE files:

```
2BFF BF00 1000 C0B8 FF00 0000
B9FF FFFF FFF2 AE8B D90B C90F
8480 0000 0081 FF00 C000 C073
```

Intercepts: Hooks IFS API OpenFile.

Payload: None.

Removal: Recover infected files from backup or replace with originals.

VIRUS ANALYSIS 2

DarkParanoid – Who Me?

Eugene Kaspersky
KAMI Associates

Computer viruses are not going to disappear. Once, we anticipated the emergence of new, protected, virus-free operating systems – an era when DOS and all its viruses, would perish. It seems we were right – DOS is becoming obsolete as an independent OS, and maybe in the near future (a century or so) it will be replaced. We were wrong too. Modern operating systems have virus-protection levels similar to those of good old DOS, i.e. they have *no* protection. Viruses have now been written for all popular OSes, including *Windows 95*, *NT*, and *OS/2*.

DOS viruses are still showing signs of development. They contain honed versions of old ideas like polymorphism and stealth, and some new tricks. Their writers may be readying these techniques for inclusion in non-DOS viruses.

There are several known tricks that viruses use to hide their code in both files and memory. The most popular is encryption, where encrypted code is decrypted when necessary. Some viruses employ several methods of encryption, including 'on-the-fly' in memory encryption, where subroutines are decrypted before execution and encrypted after it. Despite their different tricks and encryption algorithms, it is true of such viruses that at some point either their complete code, or major subroutines, are decrypted. This is not the case for the new, polymorphic virus, DarkParanoid.

Encryption

This virus uses an ultra-complex method of 'on-the-fly' encryption. At any time, only one instruction is in unencrypted form (apart from the en/decryptor code). The virus manages this by using tricks with Int 01h tracing mode. When the virus first receives control, it hooks Int 01h. Subsequently, the execution of almost all instructions causes the Int 01h code to be invoked. After executing the current instruction, DarkParanoid takes control with the Int 01h hook, encrypts the current instruction and decrypts the next one. Thus, at any given moment, either all of the virus code is encrypted, or just one instruction is clean. Moreover, the virus encrypts/decrypts the code of previous/next instructions imprecisely, as bytes/words at several offsets from the current instruction's address.

Three blocks of code cannot be encrypted at the same time – the Int 01h handler (en/decryptor), the start code in infected files, and the Int 21h handler. Both the start code and the Int 21h handler hook Int 01h on receiving control, then switch to tracing mode, passing control to the installation routine and back to the Int 21h handler, respectively.

Although the Int 01h hooking routine and the Int 01h handler itself are not encrypted, they are polymorphic. The virus uses quite a strong polymorphic engine to generate these code sequences. As a result, all entries to the virus are polymorphic, and the main code is always encrypted. It is thus quite difficult for anti-virus researchers to design detection procedures for this kind of virus.

Polymorphic Engine

The difference between an ordinary polymorphic engine and that of DarkParanoid is that in this virus there is no decryption loop in the polymorphic code – it just hooks Int 01h and starts tracing the main code. This code may appear in different forms in infected files, because while generating this code, the virus randomly selects registers, commands, data access modes and so on.

The same is true for the Int 01h handler that contains the 'on-the-fly' encryption/decryption routines. This code is also different in various files – more than ten encryption functions are randomly selected from the set: ADD, SUB, XOR, NEG, NOT, ROR, ROL, as well as byte and word access. Further random registers are used, and the Int 01h handler offset is randomly selected within certain limits.

Installation and Int 21h Handler

The rest of the virus is not so interesting. It is memory-resident, allocating a block of system memory either in conventional DOS memory, or in Upper Memory Blocks, providing there is 7.5 KB free. The virus copies its code there, hooks Int 21h and returns control to the host.

While going memory-resident, the virus runs its polymorphic engine in order to generate decryption routines for use during infection. DarkParanoid does not call this engine again, and as a result it will use the same polymorphic code up to the next reboot and re-initialization. This may fool both users and virus researchers into thinking that the virus is simply encrypted, not polymorphic, and that it is possible to detect it with a simple hex pattern.

The Int 21h handler intercepts file open, create and close functions, and the GetAllocationStrategy (AX=5800h) function. The latter is used as an 'Are you there?' call, performed by the virus while going memory-resident. Before calling this function, DarkParanoid 'codes' the current year, month and day into the CX register (by adding the CX and DX registers after calling the DOS Get Current Date function; Int 21h AH=2Ah).

If DarkParanoid is memory-resident, it intercepts the 5800h function call and compares the current date and year to those in the CX register. If they match, the TSR copy of the virus does not return control to the active virus, but passes it to the host program. This seems to be quite an effective anti-debugging trick – if the virus is already memory-resident, an ordinary call like GetAllocationStrategy will not return to the debugger.

When a file is opened, the virus compares its name extension to 'COM' and 'EXE', and on a match, saves the file's handle in order to infect it when the file closes. Thus, only executable files get infected, when they are either opened (for example, when they are scanned for viruses by an anti-virus program, or backed up), or copied. Before infecting a file, the virus checks its name. Those that begin with AV, SC, CL, GU, NO, FV, TO, TB (AVP, AVG, SCAN, CLEAN, GUARD, TBAV, etc) are not infected.

DarkParanoid writes its code to the end of EXE files and modifies the necessary fields in the EXE file header. In the case of a COM file, the virus writes its code to the beginning of the file and saves the original file start to the end.

Infection causes variable file size increases. DarkParanoid writes 5297 bytes of encrypted code to the host, in addition to a randomly-selected chunk of data (up to 1001 bytes long) from a randomly selected memory address. EXE file lengths are paragraph-aligned before infection, and COM files larger than 60 KB are not infected. It checks file headers for the MZ/ZM EXE stamp, to separate COM from EXE files. As an infection marker, DarkParanoid uses the common trick of setting the seconds field of the host's time-stamp to a fixed value – in this case two.

Trigger Routine

During infection, DarkParanoid executes a trigger based on a random counter – there is a 1 in 4000 chance of the virus displaying the text 'DaRK PARaNOiD' in the middle of the screen, followed by noises and the use of VGA features to 'shake' the screen. The virus also contains the text 'ENGINE OF ETERNAL ENCRYPTION' inside its polymorphic engine code.

DarkParanoid

Aliases:	None known.
Type:	Memory-resident, polymorphic virus that stays encrypted in memory.
Infection:	COM and EXE files.
Self-recognition in Files:	Seconds field of time-stamp set to two.
Self-recognition in Memory:	Uses Int 21h AX=5800h call, see text.
Hex Pattern:	Not possible in files or memory.
Intercepts:	Various Int 21h file functions for infection and AX=5800h 'Are you there?'; Int 01h for on-the-fly en/decryption.
Trigger:	Displays a message and 'shakes' the screen based on a random counter.
Removal:	Under clean system conditions identify and replace infected files.

COMPARATIVE REVIEW

In the Frame

It has been eight months since *VB* last published a comparative review of *Windows 95* scanners. At the beginning of 1997 there was a suspicion we may be running our first 'Which products best made the transition to *Windows 97*?' review, but the folk at Redmond have postponed our ability to run those tests for a few more months (and it will then be the 'transition to *Windows 98*' review).

As was remarked back in May, *Windows 95* and most of the products designed for it have reached a fair degree of stability and acceptance in the mainstream computer market, though many large corporate IT departments are clinging to *Windows 3.1* until making the move directly to *Windows NT*.

We received twenty packages in response to our call for products, including two new faces – *eSafe* being a souped-up and repackaged version of *EliaShim's ViruSafe* and *RAV*, from *GeCAD* in Romania, being completely new to *Virus Bulletin* tests (although the version number of 5.02a suggests it has a fair tradition in its home market). Most of the products provided the sort of initial user impression expected of contemporary *Windows 95* applications – good, easy to follow installation procedures that leave an uninstall option, progress indicators, browse buttons where they should be, context menu additions (scan drive/file/folder on right-click in Explorer) and the like. Seventeen of the twenty had a resident or on-access scanning component, but one of these could not be tested because it only detected viruses on execution of infected files and *Virus Bulletin* cannot test this detection mode.

Testing

As usual for *VB* comparatives, vendors were asked to supply the product they would sell to *Windows 95* user looking for virus protection. GUI-only anti-virus software would present a small problem in cases where *Windows 95* will not start and/or in the case of boot sector infections, where most products (rightly) refuse to disinfect the virus while it is active. The simple solution to these problems is to provide a DOS scanner for 'emergency use'. A few products take this a step further and provide their own 'emergency boot diskette'. Although these components are clearly very important should you need to resurrect an infected system, we focused solely on the 'main scanner', which in all but one case was a *Win32* GUI application.

In a break with *VB* tradition, the tests were run on three machines. Ostensibly identical, these were all built to the same specification with the same components and all hardware was configured identically (for specifications see the Technical Details box at the end of the review). Despite the machines supposedly being identical, all timed tests were run on just one of them. The operating system was installed and configured on one machine, the disk fully defragmented and free space on it filled with zeroes. A sector-level image was then made. This was implanted onto each of the other machines, where minor configuration changes were necessary (all three machines are on the test network, and thus needed different names and the like). Images were then made of the second and third machines' disks. Between installing each product for testing, the hard drive was completely rewritten from the appropriate image file, so each test started from the same point.

The common *VB* tests were run – speed (and propensity for false alarms) against the Clean test-set, speed against a clean and infected diskette, and virus detection. With the increasing use (and importance) of resident or on-access scanning, we tested the detection abilities of the products with such options. Lastly, we endeavoured to measure the performance overhead of on-access scanning.

Please note that except in the case of 100% scores and the ItW Boot test-set, taking the number of samples detected in a test-set and dividing by the total number of samples in that set can give a slightly different result from that reported. This is particularly true of the Polymorphic test-set. The results are based on a weighted calculation that corrects for the number of samples of each virus (and provides a bonus weighting for complete detection of a stem in the case of the Polymorphic test-set). A complete explanation of these calculations is available from the *VB* web site address given in the Technical Details section.

The test-sets used were updated slightly, relative to the previous comparative review. The most important changes reflected the modifications to the WildList, bringing the ItW sets up-to-date to August 1997 (the current WildList at product submission date).

On-access Tests

Both the on-access tests – detection and overhead – caused the reviewer considerable grief. Due to a range of problems across many of the products, the on-access detection tests were eventually cut back to just the In the Wild File and Macro test-sets (probably the two of most concern to our readers). We plan to run on-access detection tests of all test-sets in our next Win32 comparative (*NT* in March).

The detection tests were complicated enormously by several products not having a 'log only' option for their on-access scanner, or having one that did not work. The prospect of sitting through more than 15,000 virus detection dialog boxes, and pressing a key each time, was not very

	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil AVAST32	90	100.0%	637	98.3%	98.9%	731	98.5%	12503	96.2%	799	100.0%
Command F-PROT Pro	90	100.0%	646	100.0%	100.0%	721	97.4%	7060	49.4%	709	91.7%
Cybec VET	87	96.7%	634	98.4%	97.8%	720	96.9%	12885	97.4%	782	98.0%
Data Fellows F-PROT Pro	87	96.7%	646	100.0%	98.9%	713	96.4%	7050	50.3%	709	91.7%
Dr Solomon's AVTK	89	98.9%	646	100.0%	99.6%	723	97.4%	12939	97.7%	799	100.0%
eSafe Protect	88	97.8%	646	100.0%	99.2%	721	97.4%	12632	91.1%	779	97.9%
Eliashim ViruSafe 95	88	97.8%	646	100.0%	99.2%	721	97.4%	12632	91.1%	779	97.9%
GeCAD RAV	77	85.6%	568	89.4%	88.1%	490	65.3%	12457	94.0%	747	93.3%
H+BEDV AntiVir/95	87	96.7%	602	93.1%	94.3%	734	98.5%	9607	71.8%	714	92.7%
IBM AntiVirus	88	97.8%	646	100.0%	99.2%	736	99.5%	12500	96.2%	799	100.0%
Intel LANDesk Virus Protect	81	90.0%	619	95.7%	93.7%	646	87.2%	11762	87.1%	765	96.3%
iRiS AntiVirus	88	97.8%	645	99.7%	99.1%	733	98.6%	12480	95.1%	793	99.3%
KAMI AVP	89	98.9%	643	99.6%	99.3%	740	100.0%	12806	97.0%	799	100.0%
McAfee VirusScan	89	98.9%	646	100.0%	99.6%	728	98.5%	12941	98.7%	779	98.4%
Norman ThunderByte	90	100.0%	646	100.0%	100.0%	729	98.6%	12996	98.1%	789	99.0%
Norman Virus Control	90	100.0%	646	100.0%	100.0%	729	98.6%	13000	100.0%	782	98.7%
Sophos SWEEP	90	100.0%	646	100.0%	100.0%	732	99.0%	13000	100.0%	797	99.7%
Stiller Integrity Master	85	94.4%	574	90.8%	92.1%	609	81.9%	4582	30.3%	595	81.5%
Symantec Norton AntiVirus	89	98.9%	640	99.4%	99.2%	731	98.5%	11501	87.5%	784	99.0%
Trend Micro PC-cillin	86	95.6%	632	97.5%	96.9%	736	99.5%	12383	93.6%	769	96.5%

appealing. Fortunately, the old trick of wedging the Enter key down looked as if it would suffice. But it was not to be. Some of the products that insist on presenting a warning do so with a system-modal dialog box, or a VxD blue-screen warning. These screens have to 'see' a key press and release before yielding, so the jammed down Enter key was not a runner. We understand there can be good reasons not to suppress such warnings, but there are situations where you do not want your machine to stop dead even though your anti-virus software has found something to warn you about. A small, key-pressing robot to get around such problems in future tests might have to be added to the *VB* test-equipment armoury.

The on-access overhead tests were performed in much the same way as in the most recent *NT* comparative (*VB*, September 1997, p.10) – copying 200 executable files from the Clean test-set from one local directory to another ten times and averaging the copying times. A slight modification was made because *Windows 95* file I/O performance seems much more variable than *NT's*. To reduce the effect of this in the results, the slowest and fastest test of the ten runs were removed from each condition's results before calculating baseline times and overheads. We are still considering the design of more realistic overhead tests and stress that the results presented are indicative of a somewhat unusual activity for a 'typical workstation'.

Alwil AVAST32 v7.70 22 Aug 1997

ItW Boot	100.0%	Macro	98.5%
ItW File	98.3%	Macro on-access	n/t
ItW File on-access	n/t	Polymorphic	96.2%
ItW Overall	98.9%	Standard	100.0%

Little seems to have changed since the last review, but as *AVAST32* performed well in the past, this is not a bad thing. The In the Wild Boot detection problems mentioned in the previous *Windows 95* comparative have clearly been fixed, with *AVAST32* turning in an unbeatable 100% on this test-set. ItW File detection is slightly down on recent results – this is solely due to missing three of the *Word 8* macro viruses (Appder.A, Kompu.A and Wazzu.C) in the test-set. The latter virus and two fairly new ones (at the time of testing), Header.A and Mess.A, prevented a perfect score against the Macro test-set, and 497 Cordobes.3334 samples were missed in the Polymorphic test-set.

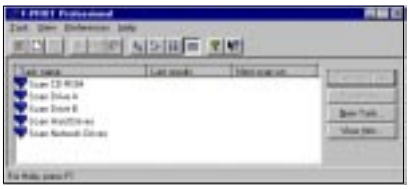
AVAST32 has an on-access scanner, but it only detects on execution and not on file open or other kinds of access. Consequently, this feature could not be tested. As the overhead test only involves executing the timing program and XCOPY ten times each, it seemed misleading to run *AVAST32* through this test.

High speed is not something *AVAST32* is noted for; in fact, it was slowest on the hard disk tests in the current round-up, taking six to eight times as long to scan the Clean test-set as its nearest rival. This may seem terrible, but it is a design feature. The developer claims that the on-demand scanner runs in a low-priority thread, and an informal test suggests that other applications do not slow down significantly while an on-demand scan grinds away in the background. Floppy scanning was also slow, placing *AVAST32* second-last on both diskette tests. Unfortunately, two false positives were registered against the Clean set.

Command F-PROT v3.00 18 Aug 1997

ItW Boot	100.0%	Macro	97.4%
ItW File	100.0%	Macro on-access	97.4%
ItW File on-access	100.0%	Polymorphic	49.4%
ItW Overall	100.0%	Standard	91.7%

With 100% In the Wild Overall detection, *Command F-PROT Professional* is one of four products to earn a VB 100% award in this review. This excellent ItW performance was maintained by its on-access scanner. Missing the two newer *Word* macro viruses Header.A and Mess.A and failing to handle *Excel* viruses other than XM/Laroux.A resulted in 97.4% detection of the Macro test-set.



Such effective detection does not extend to the Standard and Polymorphic test-sets. In fact, a score below 50% on the latter must be a little worrying. Despite being supplied with a more up-to-date scan string set than came with the *Data Fellows F-PROT Professional*, *Command's* version missed one SatanBug.5000.A sample, denying it the 'bonus' for that stem. Thus, *Command F-PROT* received a lower rating on the Polymorphic test-set than the *Data Fellows* version, even though it detected a handful more viruses (amongst the Alive.4000 samples).

Speed and overhead are an interesting trade-off with this product. At the slower end of the fastest third of scanners tested, and twice as fast as about half of the muster, you will probably not be disappointed in its on-demand performance. It also returned the fastest clean diskette scan time, which increased by half on the infected diskette test. However, its on-access overhead of about 50% puts it in the bottom third for this test, with about half the products providing noticeably less overhead. No false positives were detected in the Clean test-set.

Cybec VET v9.5.1

ItW Boot	96.7%	Macro	96.9%
ItW File	98.4%	Macro on-access	96.9%
ItW File on-access	98.4%	Polymorphic	97.4%
ItW Overall	97.8%	Standard	98.0%

Traditionally one of the faster products, *Cybec's* offering came in third fastest on the Clean set, and it correctly found no viruses there. *VET* missed three samples from the ItW Boot – the same three that caused so many products problems in the recent *NT* comparative. Interestingly, *VET* for *NT* detected those samples, which shows there is more to writing a *Win32* anti-virus program than bolting a flash GUI onto an existing detection engine. The HLLP.5850.C and .D samples added in the August WildList update, and the *Word 8* form of Wazzu.C denied *VET* 100% on the ItW File test. On-demand detection rates around 97-98% against *VB* test-sets are typical of recent *VET* performance.

In keeping with its speedy reputation, *VET* was third and fourth fastest, respectively, on clean and infected diskette scanning. An overhead of 20% on the 'read and write' condition is still better than many (nine in this test), but it is probably starting to be noticeable.

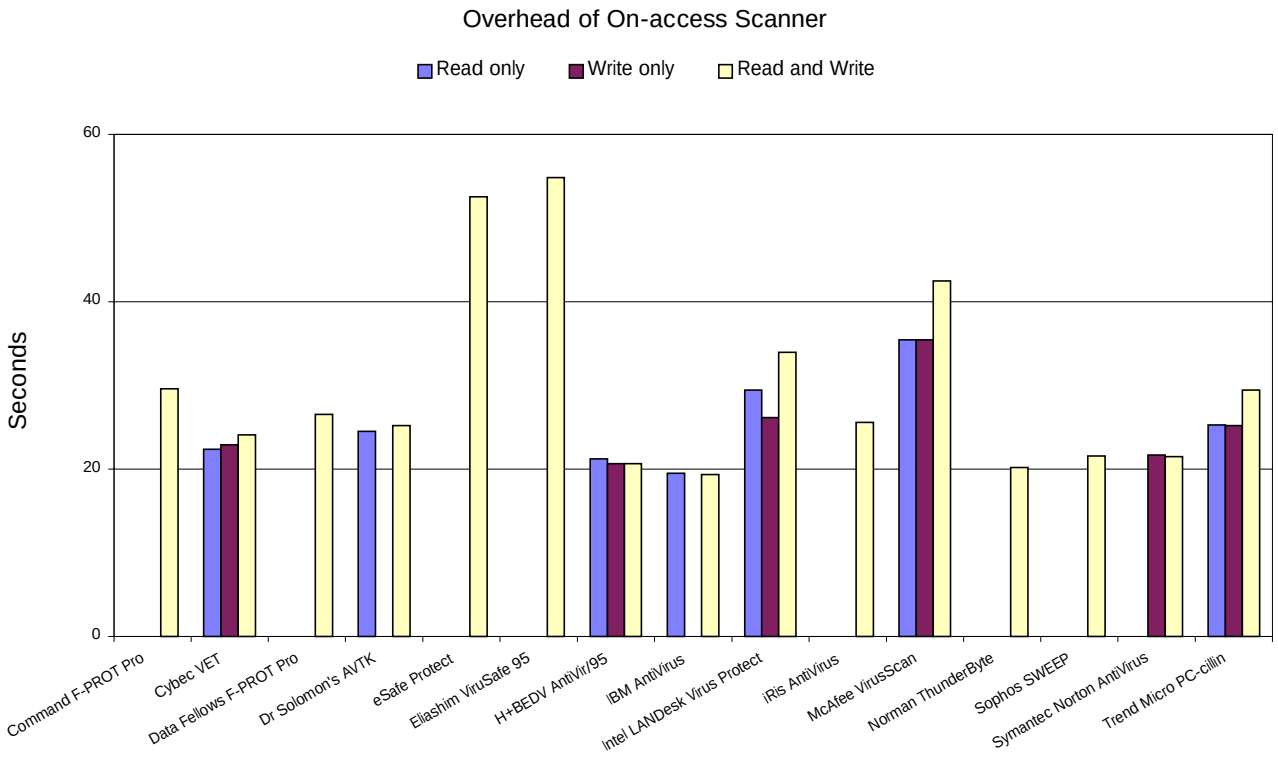
	ItW File on-access		Macro on-access		Hard Drive Speed		Clean Diskette Speed		Infected Diskette Speed		False Positives
	Number	%	Number	%	Scan time (min:sec)	Data rate (KB/s)	Scan time (min:sec)	Data rate (KB/s)	Scan time (min:sec)	Data rate (KB/s)	
Alwil AVAST32	n/t	n/t	n/t	n/t	88:48	100	1:05	15	1:12	16	2
Command F-PROT Pro	646	100.0%	721	97.4%	4:29	1986	0:21	46	0:38	31	0
Cybec VET	634	98.4%	720	96.9%	3:13	2767	0:25	39	0:29	41	0
Data Fellows F-PROT Pro	632	97.1%	707	94.9%	5:48	1535	0:27	36	0:43	27	0
Dr Solomon's AVTK	646	100.0%	740	100.0%	3:36	2473	0:32	30	0:59	20	0
eSafe Protect	638	98.9%	709	95.9%	4:10	2136	0:21	46	0:24	49	9
Eliashim ViruSafe 95	638	98.9%	709	95.9%	4:49	1848	0:22	44	0:25	47	9
GeCAD RAV	n/a	n/a	n/a	n/a	10:55	815	0:42	23	1:06	18	31
H+BEDV AntiVir/95	574	89.1%	670	89.7%	7:47	1144	0:34	29	0:40	30	6
IBM AntiVirus	504	78.9%	732	99.0%	2:05	4273	0:29	34	0:33	36	0
Intel LANDesk Virus Protect	613	95.2%	646	87.2%	10:58	812	1:19	12	1:40	12	0
iRiS AntiVirus	645	99.7%	694	94.0%	8:52	1004	0:34	29	0:39	30	16
KAMI AVP	n/a	n/a	n/a	n/a	10:16	867	0:56	17	0:46	26	0
McAfee VirusScan	646	100.0%	728	98.5%	10:26	853	0:46	21	0:54	22	0
Norman ThunderByte	646	100.0%	729	98.6%	3:05	2887	0:25	39	1:10	17	1
Norman Virus Control	n/t	n/t	725	98.1%	5:45	1548	0:41	24	0:58	20	0
Sophos SWEEP	640	99.1%	729	98.6%	5:15	1696	0:36	27	0:32	37	0
Stiller Integrity Master	n/a	n/a	n/a	n/a	4:13	2111	0:29	34	0:42	28	1
Symantec Norton AntiVirus	640	99.4%	739	99.5%	5:13	1706	0:41	24	0:57	21	0
Trend Micro PC-cillin	632	97.5%	736	99.5%	11:12	795	0:45	22	0:59	20	0

Data Fellows F-PROT v3.00 17 June 1997

ItW Boot	96.7%	Macro	96.4%
ItW File	100.0%	Macro on-access	94.9%
ItW File on-access	97.1%	Polymorphic	50.3%
ItW Overall	98.9%	Standard	91.7%

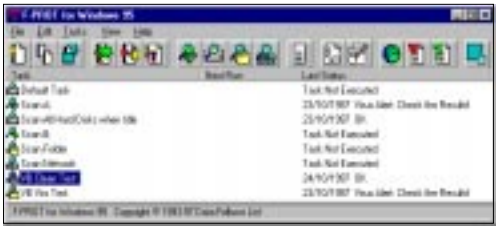
A perfect score against the In the Wild File test-set is always encouraging, but missing three In the Wild Boot viruses takes the gloss off this somewhat. Again, it was samples exhibiting the BPB problem that has been mentioned in the two previous *NT* comparatives. Soon after this product was submitted for review, *Data Fellows* informed *Virus Bulletin* that it had rectified the BPB problem with its *NT* product. Hopefully *Data Fellows* is also addressing this issue in its *Windows 95* product.

Data Fellows provided the review copy on CD-ROM, but did not supply an updated scan string set. As the CD was the June release, it seemed unlikely its results would be quite as good as *Command's* despite both products being based on the same scanning engine. Despite this, or perhaps highlighting the depth of experience and research behind the scanning engine, detection of the ItW File set matched, but perhaps not surprisingly, *Data Fellows F-PROT* scored a little lower on the Macro test-set.



The on-access tests returned slightly poorer performances than the on-demand ones. Fourteen ItW samples were missed in this test (all of the *Word 8* and *Excel 8* samples in the ItW set), as were an additional six samples in the Macro test-set (four of W97M/Nightshade and one each of W97M/Wazzu.A and .C).

On-demand scanning speed and on-access overhead were both in the middle of the pack, but quite acceptable. Floppy disk scanning speed ranked slightly higher, but was nothing to write home about. No false positives were reported against the Clean test-set. The test machine's performance was unreliable with the *Data Fellows* product installed, locking-up occasionally and trapping many exceptions.



Hopefully these stability issues will have been addressed in later releases.

Dr Solomon's AVTK v7.74 23 June 1997

ItW Boot	98.9%	Macro	97.4%
ItW File	100.0%	Macro on-access	100.0%
ItW File on-access	100.0%	Polymorphic	97.7%
ItW Overall	99.6%	Standard	100.0%

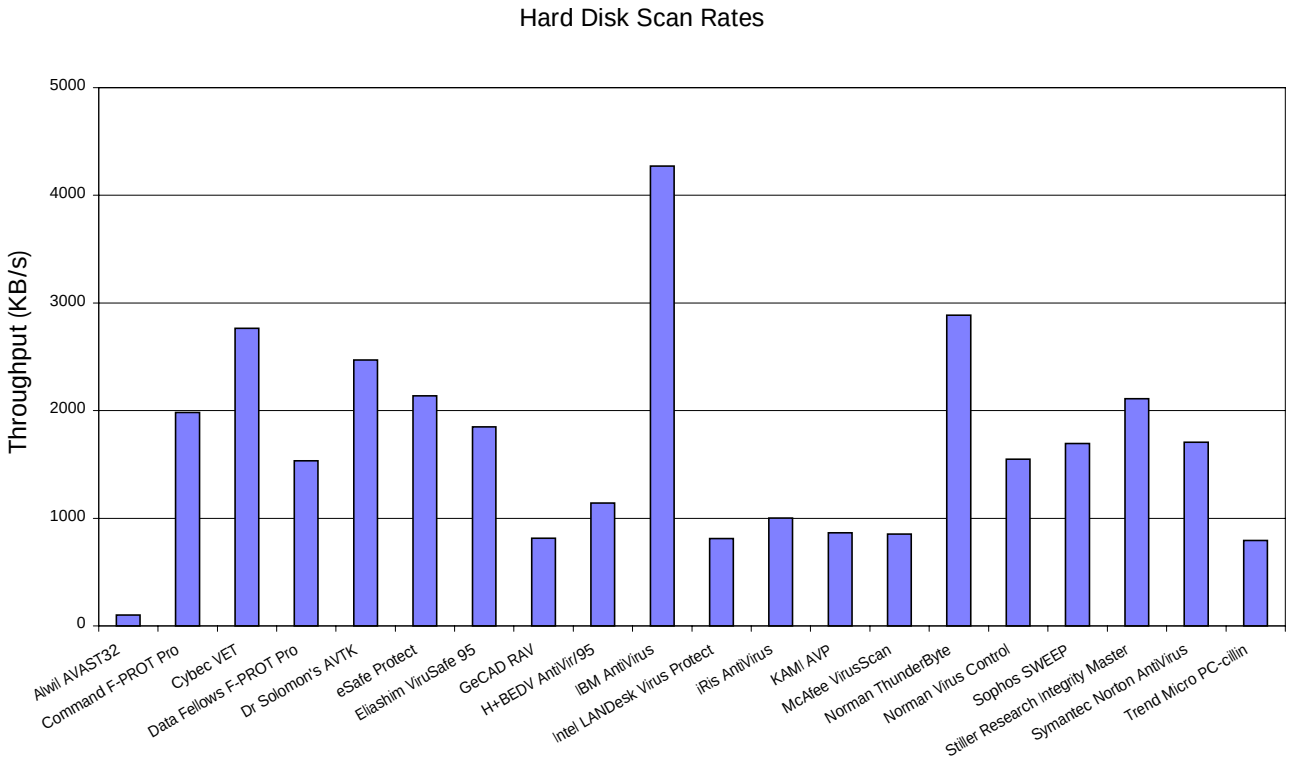
Submitting what, at the time, was a slightly outdated version of their software might have been what stood between *Dr Solomon's AVTK* scoring 100% ItW Overall and missing it by the single sample of the boot infector Moloch. However, the breadth and depth of *AVTK's* detection capability is seen in the fact that, despite its age, it detected 100% of both the Macro and Standard test-sets, and only missed 61 samples in the Polymorphic test-set.

Although not renowned as a speedster, the *AVTK* had fourth highest throughput scanning the Clean test-set, but fell fairly much mid-range on the diskette tests. Its 25% on-access overhead might not upset, but there are products with a lower impact. It was interesting that the on-access scanner detected 100% of the Macro set, bettering the on-demand scanner! Regardless, it was one of only two products to achieve 100% on this set. On-access detection of the ItW File set stayed at 100%.

The *AVTK* interface still does not 'feel' very much like a *Windows 95* program. There is not much else to say – *AVTK* gave its typically high detection and no false positives.

eSafe Protect v1.02 28 Aug 1997

ItW Boot	97.8%	Macro	97.4%
ItW File	100.0%	Macro on-access	95.9%
ItW File on-access	98.9%	Polymorphic	91.1%
ItW Overall	99.2%	Standard	97.9%



The first of the two newcomers to *VB* tests, *eSafe Protect* proclaims itself as 'the original anti-vandal software'. A product of *eSafe Technologies*, a division of *EliaShim*, *eSafe Protect* is based on the same virus scanning engine as *EliaShim's ViruSafe* (see below) but adds ActiveX and Java malware detection capabilities, and behaviour blocking. These were not tested in this review.

The on-demand scanner module looks very like *ViruSafe* with a different colour scheme and ancilliary graphics. However, the actual *eSafe* interface is quite 'exciting' (for lack of a better word). With its animations, levers and dials it would not have looked out of place on a hand-held, flip-top, hi-tech gadget in a recent movie. Although not the version submitted for review, most *VB* readers would probably be more interested in the Enterprise version, which is claimed to be geared to corporate LAN/Intranet use. *eSafe Protect's* performance was essentially identical to *ViruSafe's*, discussed below.

EliaShim ViruSafe 95 v2.1 28 Aug 1997

ItW Boot	97.8%	Macro	97.4%
ItW File	100.0%	Macro on-access	95.9%
ItW File on-access	98.9%	Polymorphic	91.1%
ItW Overall	99.2%	Standard	97.9%

As explained above, *ViruSafe* and *eSafe* both use *EliaShim's* scanning engine. As the same version and scan string set were supplied with both, it is not surprising they obtained the same results – in fact, it would be notable if they had not done so.

Missing Moloch and Hare.7750 on the ItW Boot test-set prevented both scanners from scoring 100% ItW Overall. On-access scanning missed the two *Excel* macro viruses in the ItW File set (XM/ and X97M/ versions of Laroux.A). It seemed this may have been because XL? was not in the default extension list for the on-access scanner, but adding it did not change things. Similarly, when testing the on-access component against the Macro set, both products missed four samples of each of three Excel macro viruses that were detected by the on-demand scanner. *EliaShim's* detection rate of the Polymorphics climbed slowly through 1997 and it is pleasing to see this improvement continue.

Speed and overhead are something of a mixed-bag with the *EliaShim*-engined products. Both products returned very respectable throughputs around the 2100 KB/s mark in on-demand scanning (fifth-equal) and the fastest diskette scan speeds, but quite poor on-access overhead results of about 150% (the highest overheads in our tests).

GeCAD RAV v5.02a 30 Aug 1997

ItW Boot	85.6%	Macro	65.3%
ItW File	89.4%	Macro on-access	n/a
ItW File on-access	n/a	Polymorphic	94.0%
ItW Overall	88.1%	Standard	93.3%

As mentioned earlier, *RAV* is the second of two newcomers to *VB* tests. The developers were anxious to see how their product fared against the *Virus Bulletin* test-sets and seemed to view submitting their product to our testing as a development opportunity. Although *GeCAD* has primarily targeted *RAV* at the Romanian market, the test copy was supplied as boxed packages with English versions of the software (but Romanian manuals).

RAV was one of the few products tested that did not use one of the common installation toolkits (most products tested used *InstallShield*), but it installed easily and cleanly, apparently doing everything 'right'. I found the lack of accelerator keys frustrating in places and the very roundabout manner of executing a diskette scan was frustrating. This, combined with the lack of a 'repeat' or 'multi' option for diskette scanning would be enough to deter anyone from scanning a modest number of diskettes (say a pocketful), let alone ninety. This gripe applies fairly equally to several other products whose design seems to discourage diskette scanning. With the growing use of on-access scanning the need to bulk scan a pile of diskettes may be falling off, but the need would arise should an infection become widespread (especially if it were a boot infector).

RAV employs a combination of known-virus scanning and heuristic analysis techniques and these helped it score favourably on the Polymorphic and Standard test-sets. It did not fare quite so well on the ItW sets. However, detecting 88.1% ItW Overall in the first showing of a product that has focused on a regional market is an encouraging start. The developers admitted that macro virus detection was *RAV's* weak spot, and they claimed to be working on improving this. Given this warning, it was not surprising that *RAV's* poorest detection result was against the Macro test-set.

No speed leader, *RAV* was one of five products with a throughput on the Clean set of around 800 KB/s. A couple of products were slower, but over half were notably quicker. Similar comments apply to diskette scanning speed, but with an appropriately lower data rate (around 20 KB/s). Some work needs to be done tightening up the heuristic decision mechanism, as *RAV* claimed to find 31 likely viruses in the Clean set. The developers are working on a resident scanner, but this was not shipping at test time.

H+BEDV AntiVir/95 v1.02 22 Aug 1997

ItW Boot	96.7%	Macro	98.5%
ItW File	93.1%	Macro on-access	89.7%
ItW File on-access	89.1%	Polymorphic	71.8%
ItW Overall	94.3%	Standard	92.7%

A dramatic improvement in ItW Boot detection, compared with recent *VB* reviews, put *H+BEDV's* ItW Overall score back into the mid-nineties. A detection rate of 98.5% against the Macro test-set is a good result, and an encouraging improvement compared to *H+BEDV's* result against this test-set in the most recent NT comparative. It is pleasing to see *AntiVir's* gradual improvement against the other test-sets still continues.

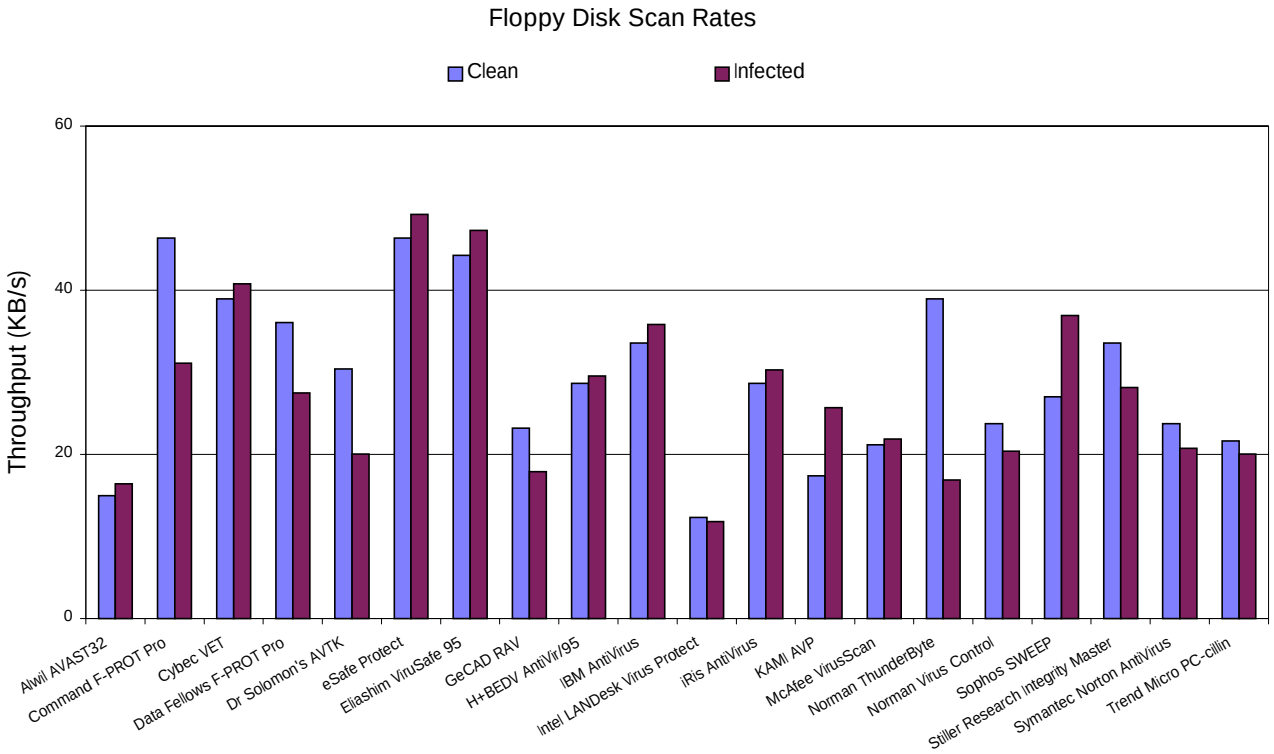
AntiVir/95's on-demand performance was middle of the pack on both the hard disk and diskette speed tests, but this is admirably compensated for by an overhead of only 5%. The on-access scanner does not detect all of the viruses the on-demand one does, but its low overhead is fairly constant, regardless of configuration. Reporting six viruses in the Clean set puts a kink in the results however.

IBM AntiVirus v3.0f

ItW Boot	97.8%	Macro	99.5%
ItW File	100.0%	Macro on-access	99.0%
ItW File on-access	78.9%	Polymorphic	96.2%
ItW Overall	99.2%	Standard	100.0%

The boot virus test-set continued its record of causing problems for Win32 scanners in denying *IBM AntiVirus* (*IBMAV*) a 100% ItW Overall score. Apart from missing Michelangelo.A and MISiS on the In the Wild Boot test, *IBMAV* missed only two other viruses from the rest of the *Virus Bulletin* test-sets – four samples of the new WM/Header.A and the Cryptor.2582 stem from the Polymorphic set. This is an impressive result.

The on-access component of *IBMAV*, called System Shield, does not provide the same detection as the on-demand scanner. Four samples of the relatively new *Word* virus (WM/Mess.A) were missed by System Shield, as were 142 samples (covering 38 viruses) from the ItW File set. By default, System Shield is configured to intercept 'execution'. File-open calls count as 'execution' for OLE2 files (*Word* and *Excel* documents), but a



load-and-execute is required for it to detect program viruses. To run a meaningful test without the risk of executing infected programs, System Shield was set to monitor all file accesses. Interestingly, the warning that this option may slow the machine down was unduly pessimistic, as both System Shield conditions resulted in slightly faster, rather than slower performance!

Another notable *IBMAV* result was its scanning speed. *IBMAV* uses integrated checksumming. After scanning a file the first time and ensuring it is not infected, *IBMAV* records a partial checksum of it. This is quickly calculated when the file is accessed again, compared with the stored value, and if the two match, the file is not be re-scanned. This makes subsequent scans of files that seldom change (most programs) very fast. Our current tests do not address performance issues with regularly changing files, such as *Word* documents.

The scan speeds presented here are based on the second scan of the Clean test-set – the first scan took almost exactly eight times as long, and would have placed *IBMAV* second slowest. This sort of scan time will be experienced on an initial install and subsequent scan string updates. *IBMAV* was in the top third of performers on the diskette speed tests, and recorded no false positives.

Intel LANDesk Virus Protect v5.0 VPN 317

ItW Boot	90.0%	Macro	87.2%
ItW File	95.7%	Macro on-access	87.2%
ItW File on-access	95.2%	Polymorphic	87.1%
ItW Overall	93.7%	Standard	96.3%

Showing a large improvement against the Standard test-set (from 71.4% in May 1997), *Intel LANDesk Virus Protect* is holding its own against the Polymorphic and Standard test-sets, but has slipped somewhat against the In the Wild Boot and File sets. Despite an improvement against the Macro test-set (compared to its *NT* stablemate in the September 1997 comparative), a detection rate of 87.2% on this test is likely to be considered too low by many.

Trailing the pack on diskette scan rates and falling in the group of five with approximately 800 KB/s on the hard drive throughput test, you would be unlikely to choose this product for its speed.

Ranging from 30% to 70%, depending on configuration, *Virus Protect's* on-access overhead is not the most daunting in the test, but falls in the bottom third of products in this regard. It detected the same viruses from the In the Wild File test-set using either method, but its on-access component missed six samples from the Macro test-set that the on-demand scanner detected.

Having the unusual option to set scanning exclusions by virus name, the cynical might assume that *Virus Protect* has a problem with false positives (what other good reason could there be for this option?), but there was no evidence of this in testing against the *VB* Clean test-set.

iRiS AntiVirus v22.01 3 Sep 1997

ItW Boot	97.8%	Macro	98.6%
ItW File	99.7%	Macro on-access	94.0%
ItW File on-access	99.7%	Polymorphic	95.1%
ItW Overall	99.1%	Standard	99.3%

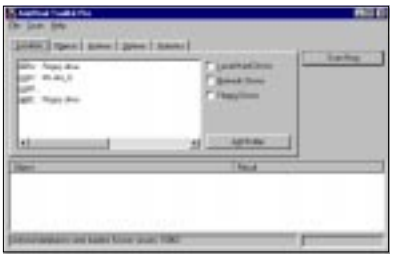
Still striving for a 100% In the Wild Overall score, *iRiS AntiVirus* missed by two boot sector viruses and one of two No_Frills_Dudley samples in the ItW File set. The product's failure to generate a useful log file regardless of which combination of settings was tried nearly resulted in it recording a 'did not complete' in the on-demand Macro test. A patient afternoon's investigation uncovered the fact that the program was hanging when trying to scan the WM/Rapi.B sample. Removing this from the test set (and counting it as a miss – only fair for all that work!) showed an otherwise good result of 98.6%. A small improvement is noted against the Polymorphic set.

The on-access component achieves the same detection rate against the In the Wild File set as the on-demand scanner, but misses 39 samples from the macro set that are detected on-demand. The on-access overhead of around 27% puts it in the company of such products as *AVTK*, *Data Fellows F-Prot* and *VET*. Hard disk and floppy scanning speeds were middle of the pack. *iRiS AntiVirus* raised sixteen false alarms against the *VB* Clean test-set.

KAMI AVP v3.0.114 2 Sep 1997

ItW Boot	98.9%	Macro	100.0%
ItW File	99.6%	Macro on-access	n/a
ItW File on-access	n/a	Polymorphic	97.0%
ItW Overall	99.3%	Standard	100.0%

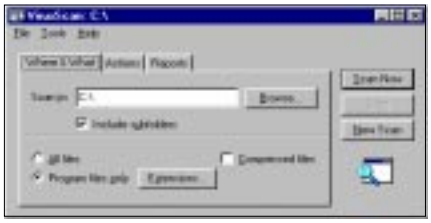
Returning excellent detection on all test-sets is the expected behaviour of *AVP*. While the detection rates lapsed slightly as the developers focused on producing non-DOS versions of the program, it looks as if the job of recovering from the slipping detection rate is all but complete. *KAMI's* scanner was one of only two to post 100% detection against the Macro test-set. As for scanning speed, *AVP* was one of the 800 KB/s group and was third slowest on the clean diskette test. It was markedly faster on the infected diskette, however, falling squarely in the middle of the field on that test.



The interface does not seem to have changed much since the previous *Windows 95* comparative, however, with the full version you now get an emergency boot disk. There is no on-access scanning component to *AVP*.

McAfee VirusScan v3.1.1 19 Aug 1997

ItW Boot	98.9%	Macro	98.5%
ItW File	100.0%	Macro on-access	98.5%
ItW File on-access	100.0%	Polymorphic	98.7%
ItW Overall	99.6%	Standard	98.4%



Compared to its excellent showing in the previous *Windows 95* comparative, overall detection has slipped very slightly, but a product detecting 100% of the ItW File set and more than 98% on all test-sets cannot be ignored. All that prevented *VirusScan* scoring 100% ItW Overall was Stoned.Daniela.

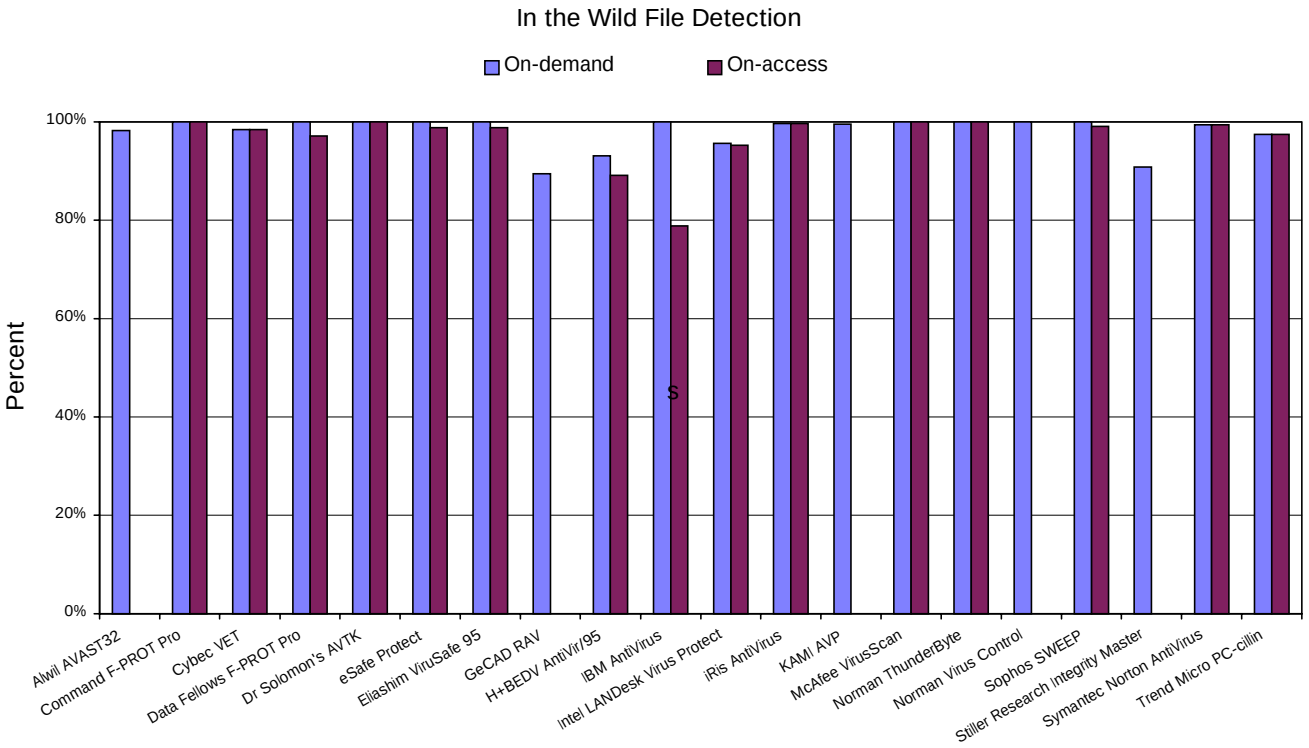
VirusScan's on-access scanner matches detection of its on-demand one – a design goal one would have thought easy to achieve, but which only three other products achieved. Maybe it is naive to expect that on-access and on-demand detection rates should match?

VirusScan's speed is towards the bottom of the field now, being one of the approximately 800 KB/s scanners on the hard disk test and 20 KB/s scanners on diskettes. It correctly failed to find any viruses in the Clean test-set. Its on-access scanner introduces a higher overhead than all others tested except those based on the *EliaShim* engine. As we have commented before, the elegantly simple interface, similar to Find Files makes the on-demand scanner very easy to use, which is an attraction of this product.

Norman ThunderByte v8.03 1 Sep 1997

ItW Boot	100.0%	Macro	98.6%
ItW File	100.0%	Macro on-access	98.6%
ItW File on-access	100.0%	Polymorphic	98.1%
ItW Overall	100.0%	Standard	99.0%

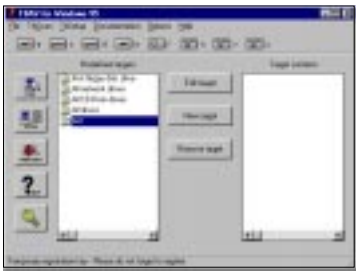
Despite its relatively poor showing in the previous *Windows 95* review, *Norman ThunderByte Virus Control* (whew – let's call it *NTVC*) is a product almost expected to produce a string of



100% scores, and it did not disappoint on this outing. *NTVC* is the second of four products in this review to attain a 100% ItW Overall rating, hence earning a VB 100% award. The macro viruses missed were the four samples of the relatively new WM/Header.A and WM/Mess.A, and three of the XM/Robocop.A samples.

NTVC's on-access component is either on or off, and is claimed to monitor all file I/O. This is not enabled by default. The performance impact of enabling this option was very low, however, returning a probably imperceptible 0.8% overhead. The File I/O Monitor returned the same detection results against the ItW File and Macro test-sets, as did the on-demand scanner.

An interesting feature of *NTVC* is the scheduler that runs background scans of your hard drive(s) at preset intervals.



Renowned for its speed, it was not surprising that *NTVC* had the second highest through-put when scanning the Clean test-set. This was tarnished somewhat by it finding one false positive in the set.

Norman Virus Control v4.20 28 Aug 1997

ItW Boot	100.0%	Macro	98.6%
ItW File	100.0%	Macro on-access	98.1%
ItW File on-access	n/t	Polymorphic	100.0%
ItW Overall	100.0%	Standard	98.7%

Another *Norman Data Defense Systems* product, *NVC's* recent test history suggested it should perform as well as *NTVC*. As the third recipient of a VB 100% award, it was not to disappoint. A low score of 98.1% against the Macro test-set (with the on-access component) would be the envy of most developers, and *Norman's* consistently high performance on our tests is a credit to their research and development efforts.

NVC's scanning speed is in the middle of the pack on the hard drive test and it places a little lower on the diskette test. The on-access scanner was only tested against the Macro set and the macro viruses from the ItW File set (the latter result is not in the results table).

The on-access protection provided with *NVC* is somewhat different from that of most other products. It consists of several components. Cat's Claw is a 'traditional' on-access scanner that only knows about macro viruses. The Smart Behaviour Blocker only intercepts load-and-execute calls and could not be tested (see the discussion of this in the section on *Alwil's AVAST32*). Cat's Claw missed the *Word 6/7* virus Hiac.A and the DOT form of Concept.J from the ItW File set, and apart from the samples the on-

demand scanner missed, all Swlabs.G samples from the Macro set. As none of the files that are copied around in the overhead test were of DOC or XLS type, it seemed publishing an overhead test, in which Cat's Claw would have been all but idle, would be misleading.

Sophos SWEEP v3.01a 1 Sep 1997

ItW Boot	100.0%	Macro	99.0%
ItW File	100.0%	Macro on-access	98.6%
ItW File on-access	99.1%	Polymorphic	100.0%
ItW Overall	100.0%	Standard	99.7%

The fourth and final VB 100% award in this review goes to *Sophos' SWEEP*. Showing form similar to recent tests, *SWEEP* was one of only three products to detect 100% of the samples in three of the five *VB* test-sets (*Dr Solomon's AVTK* and *Norman Virus Control* being the others).

Somewhat surprisingly, the on-access component detected slightly fewer viruses in the ItW File and Macro tests. On examination, the misses were all DOC forms of *Word 8* macro viruses.

SWEEP's scanning speed is middle of the pack on both hard drive and diskette tests, although its infected diskette scan was noticeably faster than its clean diskette scan. The high detection rate is coupled with a low on-access scanner overhead of around 10%. As one would hope, no viruses were reported in the Clean test-set.

Stiller Research Integrity Master v3.21a

ItW Boot	94.4%	Macro	81.9%
ItW File	90.8%	Macro on-access	n/a
ItW File on-access	n/a	Polymorphic	30.3%
ItW Overall	92.1%	Standard	81.5%

It should come as no surprise that *Stiller Research* submitted their DOS-based product for review. The integrity checking part of *Integrity Master* is well-regarded, and apart from the user-interface 'niceties', there is probably no compelling reason to implement a GUI version of the product. That said, this review focuses on virus scanning and *Integrity Master* looks somewhat odd in the line-up.

The first stage of installing an integrity management system is usually to confirm the integrity of the things to be managed – it is generally not desirable to ensure the integrity of something that has already been compromised! Thus, *Integrity Master* includes a virus scanner, which we tested. A score of 92.1% In the Wild Overall is disappointing, given the significance of the task *Integrity Master's* scanner is charged with. One would especially hope that all boot viruses thought to be in the wild would be detected.

That said, the flip side is (at least for file infectors) that a good integrity checker should spot any modifications due to subsequent infections from a virus that was missed by the pre-install scan. However, you may have to obtain another scanner or wait for *Stiller Research* to get an update to you to detect the source of these infections. Similar back-and-forward claims could be made about misses on any of the other test-sets.

Hard disk scanning speed is quite acceptable, ranking approximately a third of the way through the list. *Integrity Master* placed about mid-field on the diskette scanning tests, being a little faster on the clean diskette than on the infected one. Unfortunately, it also registered one false positive against the Clean test-set.

Symantec Norton AntiVirus Build 26J

ItW Boot	98.9%	Macro	98.5%
ItW File	99.4%	Macro on-access	99.5%
ItW File on-access	99.4%	Polymorphic	87.5%
ItW Overall	99.2%	Standard	99.0%

The software submitted for review was a pre-release copy of the eventual v4.0. It seemed fully functional except that the About option on the Help menu did nothing. The test results are interesting, showing slight slippage on both In the Wild test-sets.

More importantly, however, *Norton AntiVirus* (*NAV*) showed excellent gains against the Standard test-sets and a small improvement on the Macro test. These improvements are in no small part attributable to the inclusion of *Symantec's* fancifully-named heuristic code analyser, Bloodhound (the report files contained many instances of 'infected with

the Bloodhound.ResCOM virus' and the like). Bloodhound did not significantly improve things against the Polymorphic test-set.

The on-access component detected slightly more macro viruses than the on-demand scanner, finding the four samples of both Word 6/7 viruses NJ-WMDLK1.A and Spiral.A. *NAV's* scanning speed was about middle of the pack on both the hard disk and diskette tests. On access overhead of 10% certainly puts *NAV* in the interesting part of the spectrum if system performance is important to you. It is encouraging that inclusion of Bloodhound's heuristics did not result in *Norton AntiVirus* reporting any false positives in the Clean set.

Trend Micro PC-cillin v3.00 VPN 323

ItW Boot	95.6%	Macro	99.5%
ItW File	97.5%	Macro on-access	99.5%
ItW File on-access	97.5%	Polymorphic	93.6%
ItW Overall	96.9%	Standard	96.5%

Evolving to major version three, *Trend Micro* has dropped the year from the product name, but little in *PC-cillin's* interface seems to have changed since the last *Windows 95* comparative. Detection of whole new classes of (potential) Internet-borne nasties, such as hostile Java and ActiveX applets, has been added, but for now these remain untested by *VB*, as does the Eudora Scan Mail plug-in.

PC-cillin's In the Wild detection has slipped slightly relative to the previous *Windows 95* and recent *NT* comparatives, missing some of the newly-added samples. It was one of the few products to detect both of the new

macro viruses in that test-set (Header.A and Mess.A), and only the somewhat surprising miss of four Concept.W samples prevented it from registering 100% detection against the Macro test-set. Aside from the slight slip in ItW detection, *Trend's* recent efforts to catch up with the better-established names continues to show with improvements against the other test-sets.

PC-cillin is not the most dynamic of performers. It falls in that group of five products towards the bottom of the stakes, with throughput ranging around 800 KB/s on the clean hard disk test and 20 KB/s on the floppy disk test.

On-access detection was identical to the on-demand result. The Read and Write test condition is effectively *PC-cillin's* default on-access scanning configuration. However, with 50% overhead you may well be tempted to use the 'advanced' configuration options to set on-access scanning to monitor only reads or writes, reducing the overhead to a more acceptable 25%.

Conclusion

So, after reading all this, which product is best? What should you buy? And why does *Virus Bulletin* not rate products with rows of shiny blobs?

Taking up the last question first, we could have reviewed the features by reading the boxes and the reviewers' guides some products included. We could have decided that 96.6% against the Macro set was a four-blob effort and 96.7% or better a five-blob one, and so on. Fortunately, *VB* readers are *VB* readers for precisely the reasons we do not do this.

You know the average age and performance of your PCs, the management and policy guidelines you have to work to, the likely risks in your organization and the 'acceptable risk' this all adds up to. You will also be aware of the strengths and weaknesses of your current anti-virus strategy and, our results will help you to make a better informed decision on which product to use.

It is pleasing to see the regularly-tested products maintaining or slightly improving their overall detection rates, and we will follow the fortunes of the newcomers with interest in subsequent *Virus Bulletin* tests.

So, where do you start? Look at the products that had 100% detection in both In the Wild test-sets and very high Macro detection. If none of these fill your other requirements, products scoring 95% or more, consistently, across test-sets and across reviews should be worth considering. With the continual increase in virus numbers, a single test result is not as important as the vendor's long-term commitment to product development and success in maintaining the level of defence its product provides.

Technical Details

Test Environment: Three 166 MHz Pentium-MMX workstations with 64 MB of RAM, 4 GB hard disk, CD-ROM drive and a 3.5-inch floppy, running *Windows 95*. These were networked to a *NetWare 3.12* server, running on a *Compaq* Prolinea 590 with 80 MB of RAM and 2 GB hard disk. The workstations could be rebuilt from disk images and the test-sets were held in a read-only directory on the server. All timed tests were run on just one workstation and it was not connected to the network for the duration of the timed tests.

Speed and Overhead Test-sets: Clean floppy: 43 COM/EXE files, occupying 997,023 bytes on a 1.44 MB diskette. Infected floppy: The same files infected with Natas.4744, occupying 1,201,015 bytes on a 1.44 MB diskette. Clean Hard Disk: 5500 COM/EXE files, occupying 546,932,175 bytes, copied from CD-ROM to hard disk. The overhead test-set is the first 200 files from the CD-ROM, occupying 21,242,293 bytes.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/Test-sets/. A complete description of the results calculation protocol can be found at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

PRODUCT REVIEW 1

Norton AntiVirus v4.0 for NetWare

Martyn Perry

This month we take a look at the new *NetWare* version of *Symantec's* well-known *Norton AntiVirus (NAV)*. The standard *Symantec* licence provision applies – if *NAV* is used 80% of the time in a business context, then it may be used free of charge in the home.

Presentation and Installation

The CD-ROM package contains program and support files for all *NAV's* different client versions. The documentation is also supplied in *Adobe Acrobat* format (PDF), together with the reader software. The SYS: volume of the target server must be mapped to a drive letter before the setup program commences. Initially, the installation process scans for any viruses in memory and then prompts for user and company names for registration purposes.

Setup provides two options – an Automatic installation, including the *Windows* configuration program (default) or a Custom installation. The Custom option lets you choose either the server module (virus protection engine) or just the *Windows* configuration program.

I chose Automatic installation for this review. At this point a useful facility checks the available disk space both locally and for any mapped drive. The target server directory (default \\server\SYS\SYSTEM\NAVNLM) must be specified and then there is a location request for the configuration program which is recommended to be on the local machine (default C:\NAVNLM). The installation proceeds by copying the required files from the CD. There is an opportunity to add a line to the AUTOEXEC.NCF file to load the NAV.NLM at server start-up. All that remains is to install any updates to the virus signatures.

NAV for NetWare

On starting the *NAV* NLM, a status screen on the server console shows the condition of the various scan modes. There are options to start or stop a scan, enable or disable the NLM, and to unload the NLM. No other options are available at the console – detailed administration is performed at a workstation running NAVNLMW.EXE.

The usual three modes of operation – Immediate, Scheduled and On-access – are provided, as is a facility specifically for handling macro viruses. A number of configuration options common to all three modes include the selection of Macintosh as well as DOS files, the selection of all files or program files, and the selection of default file extensions.

Out of the box *NAV* is set to scan files with extensions of ADT, CBT, CLA, COM, CPL, DLL, DOC, DOT, DRV, EXE, OV?, PPT, SCR, SYS, and XL?.

A comprehensive range of file exclusions can be defined by file name, extension, directory and subdirectory, with predefined exclusions for SYS:\SYSTEM\NET$*.SYS and CONFIG.SYS. Further exclusions can be defined based on users or groups of users, and these can be enforced permanently or for a specified period. All scan modes have the option of scanning for unknown viruses (i.e. running *Symantec's* Bloodhound heuristic analyser). Regardless of your choice though, heuristic scanning occurs if enabled on the Heuristics configuration page. I left this option set at the default of Minimum for the main tests.

Scanning

The extent of an Immediate scan may be defined from server level down through directories and subdirectories to individual files. Immediate scans are started and stopped either from the administration program or from the server console. Maximum CPU usage can be configured so that the scanner does not hog CPU resources. While testing, I left this at the default setting of 100%.

On-access scanning can be set for incoming file checks, outgoing file checks, a combination of both or none at all. In addition, DOS and NLM memory may be checked. The On-access configuration can be propagated to other servers if required. Scheduled scans have much the same configuration options as the other types, and many schedules can be defined. An additional option for Scheduled scans is to load another NLM (such as backup) on scan completion. The frequency options are One Time Only, Hourly, Daily, Weekly or Weekdays. If a virus is detected during a Scheduled scan, you can use the existing Default Alert settings or customize settings to suit. The latter option includes sending alerts to the standard alert destination, the file user or owner and to the console. This can be very useful for out-of-hours operation. It is possible to predefine multiple Scheduled scans, but they cannot activate until they are enabled individually in the option list.

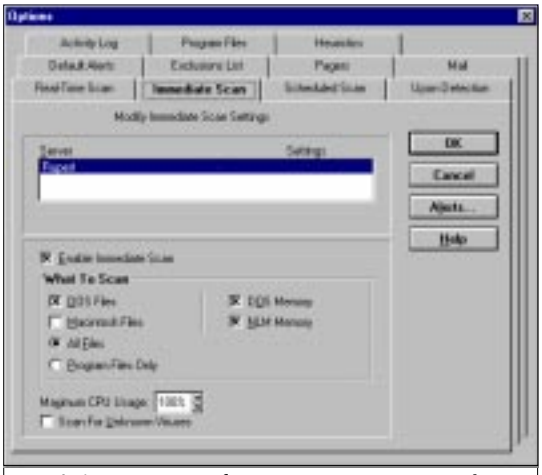
All three scan modes have the same activity options upon detection – they attempt to repair a file or macro virus. If that repair fails, then the file may be set to deny user access, or may be purged, renamed with a user-defined extension, or moved to a user-defined directory. Additional options allow loading another NLM and forcing the workstation to logout. Separate actions apply to detection of unknown viruses. Here the choice is either to ignore or inoculate (checksum) the affected file. This may be necessary following software upgrades, where the new files do not match an existing checksum.

Administration and Reports

The scanner configuration options can only be set from the *Windows*-based administration program. The limited functions that are available from the server console are also available from the administration workstation.

The appropriate password must be used to access the administration software. Each server under the Administrator's control is viewable, as is the status summary of each mode. A useful feature allows you to set the options in the three scan modes without having to execute them immediately – they can be pre-defined by a master administrator and activated by a different administrator later.

It is possible to tune the log file to handle one or more of the following events – Known Virus, Unknown Virus, Start/End Scan, Load/Unload NLM, Virus List changes, From Workstations (when a virus is detected on a workstation running *NAV*), NLM status, and error messages. The log file size can be limited (default 100 KB). Considering the amount of data that logging can generate, it is advisable to use a date filter, as well as those filters which view the events listed above.



NAV's extensive configuration options are set in this dialog in the *Windows*-based administration program.

Logs can be printed or saved to a user-named text file. In addition to the activity reports, a very useful Configuration Report provides status reports for each server, detailing the setups for each scan mode, and modem setups for alerts.

Alert Management and Support

Alerts can be broadcast to the file user, owner, or updater, the system console, system administrator, all users, specific users or user groups. They can reach various destinations using facilities such as Pagers or via email using MHS. Since all administration activities are controlled from the *Windows* administration program, there are no command-line options. This is provided by installing the appropriate workstation version of *NAV* and ensuring that workstation alerts are configured under the administration program.

Aside from providing known-virus scanning, a checksum facility, rather misleadingly labelled as 'inoculation', may be applied to various items from a whole server down to types of files or individual files. Further, the Administrator can remove individual checksums if needed.

Macro Virus Protection (MVP) Technology

With the ever-increasing threat posed by macro viruses, *Symantec* has added a macro management facility to *NAV*. MVP requires the *NAV* administrator to maintain a list of 'approved macros' for *Microsoft Word 6/7*, *Word 97*, and *Excel 97* documents. Alternatively, all macros for a specific document type can be 'disapproved'. Whenever a document is scanned – either on-demand with the *NAV* scanner or by *NAV* Auto-Protect – all non-approved macros are stripped from the document, hopefully eliminating infections from unknown macro viruses.

To create the list of approved macros, the MVP Definition Compiler (MVPDEF.EXE) processes documents identified as containing approved macros. The MVPDEF is a command-line driven utility, possibly seeming a little out of place in today's GUI world, but as it is intended for system administrator use, it may not be too daunting.

The MVP Definition Compiler generates two files in the folder from which it runs. MVPDEF.DAT (the MVP definitions data file), must be copied to workstations running *NAV*. It allows approved macros to be identified by name and the CRC of their code. All macros are 'approved' by *NAV* in the absence of this file. The other file MVPDEF produces is a text file containing a summary of the files processed, the macros they contained and the products they are from. There is a limit of 1024 approved macros per *Microsoft* product. This may be on the low side for a large organization.

When a macro that is not on the approved list is detected during the regular course of *NAV's* operation, it reports 'UNAPPROVED MACRO.' If the user site is not configured to Repair Automatically, you are instructed to choose Repair, which deletes the macro.

Updates

The 01/12/97 virus definitions were supplied for review, claiming knowledge of 12,793 viruses. Signature updates can be taken from the Internet using LiveUpdate or from diskette. Updated signatures are extracted and stored on a master server. Other servers can be automatically updated from there if you administer *NAV* on more than one server.

Detection

The *NAV* scanner was checked against the In the Wild File, Macro, Polymorphic and Standard test-sets. Files detected as infected were deleted. The results were good, with 100% success against the Macro test-set, while six samples of HLLP.5850.D from the In the Wild File set and fifteen samples across four families in the Standard test-set were missed. The main problem was missing three sets of polymorphic viruses. All Baran.4968 and Mad.3544, and 497 of 500 Cryptor.2582 samples were missed.

The heuristic scanning option mentioned earlier has been added since I last tested *NAV*. The three Cryptor 'detections', and several in the Macro and Standard test-sets, were due to the heuristics engine. To test its ability to detect unknown viruses further, a full heuristic scan was run on those missed at the default setting of minimum heuristics.

It found one more Anarchy.6503 infection and 344 of 496 previously-missed Cryptor.2582 samples, but still missed all Baran.4968 and Mad.3544 samples. Although this additional check provided some extra detection, the full heuristic test is slow. It took almost as long rescanning the undetected 1520 files as it took to scan the full set of 15,164, and the CPU load was significantly higher.

Real-time Scanning Overhead

To determine the impact of the on-access scanner on the server, the following test was executed. The basis of the test was to time the copying of 63 files of 4,641,722 bytes (EXE files from SYS:PUBLIC) from one server directory to another using *Novell's* NCOPY. Using NCOPY keeps the data transfer within the server itself, minimizing network effects. The directories used for the source and target were excluded from the virus scan so as to avoid the risk of a file being scanned while waiting to be copied.

Due to the different processes which occur within the server, the tests were run twenty times for each setting and an average taken. The test conditions were:

- NLM not loaded. This establishes the baseline time for copying the files on the server.
- NLM loaded; In = No, Out = No, Scan = No. This tests the impact of the scanner loaded in its quiescent state with no real-time or immediate scan in progress.
- NLM loaded; In = Yes, Out = No, Scan = No. This shows the overhead when scanning incoming files.
- NLM loaded; In = No, Out = Yes, Scan = No. This shows the overhead when scanning outgoing files.
- NLM loaded; In = Yes, Out = Yes, Scan = No. This shows the overhead of having both read and write scans in effect.
- NLM loaded; In = Yes, Out = Yes, Scan = Yes. This shows the incremental effect of running an immediate scan in addition to the real-time scan.
- NLM unloaded. This is run after the other tests to check how well the server returns to its former state.

The initial impact of loading the scanner software is minimal. There seems to be a significant difference in overhead between incoming and outgoing checks. Clearly, different processes are occurring between incoming and outgoing checks which are not immediately apparent. The minimal residual overhead, when NAV.NLM is unloaded, is due to CLIB and STREAMS NLMs remaining loaded on the server. The detailed results are in the product summary box. [*According to* Symantec, *the scan-caching technology in both* NetWare *and* NT *server products, should, over time, see overhead reduce dramatically for frequently accessed files. We were unable to test this claim. Ed*.]

Conclusion

NAV provides a good range of configuration options for all scanning modes with easy deployment to multiple servers. Its extra facility for handling macros is a creative response to an ever-growing problem. Detection results were mixed across the test-sets, with polymorphics faring quite poorly. The additional selection of heuristic detection did little to improve the overall detection rate. Although the extra workload is to be expected when heuristics are selected, the additional overhead makes it an unlikely option, except possibly for out-of-hours scheduled scanning.

Obviously there is much more activity involved with incoming than outgoing files, but the on-access overhead seems inconsistent. Overall, *NAV v4.0 for NetWare* maintains the standard expected from *Symantec*, but it would benefit from some speed improvement in its heuristics.

Norton AntiVirus v4.0 for NetWare

Detection Results

Test-set[1]	Viruses Detected	Score
ItW File	643/649	99.1%
Standard	784/799	98.1%
Macro	716/716	100.0%
Polymorphic	11501/13000	88.5%

Overhead of On-access Scanning:

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

	Time	Overhead
NLM not loaded	3.2	–
NLM loaded, inactive	4.9	53.1%
— + enabled + scan incoming	60.1	1778.1%
— + — + scan outgoing	6.7	109.4%
— + — + scan both	60.3	1784.4%
— + — + — + on-demand scan	62.1	1834.9%
NLM unloaded	3.4	6.3%

Technical Details

Product: *Norton AntiVirus v4.0 for NetWare.*

Vendor: *Symantec UK Ltd*, St. Cloud Gate, Maidenhead, Berkshire SL6 8XD, UK. Tel +44 1628 592222, World Wide Web http://www.symantec.com/nav/.

Price: £469 for a single server. Volume licensing should be discussed with Symantec Corporate Sales.

Hardware Used: Server: *Compaq* Prolinea 590, 80 MB of RAM, 2 GB hard disk, running *NetWare 3.12*. Workstation: 166 MHz Pentium-MMX, 64 MB of RAM, 4 GB hard disk, CD-ROM drive, 3.5-inch floppy, running *Windows 95*.

[1]**Test-sets:** See *VB*, September 1997, p.16.

PRODUCT REVIEW 2

Norman Virus Control v4.30 for Windows 95

Dr Keith Jackson

The last time I reviewed *Norman Virus Control (NVC)* for *VB* was in May 1994. *Norman Data Defense Systems* alleges that *NVC's* scanner 'can now detect and remove all known macro viruses… '. It makes the same claim of its memory-resident scanner. These are bold words, and I tried to test the product against them. There are versions of *NVC* for *OS/2*, *Windows 3.1x*, DOS, and *NT*. It also claims to work successfully in a network, but this review only covers version 4.30 for standalone *Windows 95*.

Installation

NVC was provided for review on three 3.5-inch, 1.44 MB floppy disks, plus one hurriedly-added floppy which provided the latest upgrade to the main executable file. On running SETUP.EXE, memory is scanned first. After displaying the licence details (does anybody actually read these?), the user's name and company were requested. A scan of the entire PC was then executed (it can be skipped, but is rightly recommended), and then a choice was offered between a Typical and a Custom installation. I chose the Custom option. After nominating the subdirectory for *NVC's* files, and the folder for its short cuts, we were off.

A typical *Windows 95* installation procedure followed, with its attendant vertical bar-graphs, etc. Suggested alterations to AUTOEXEC.BAT are only made if you agree to them (which is good), and the README file is displayed, if you wish, when installation is complete. Installation of *NVC* ran to completion without ever requesting the third and last disk, which is odd. [*The developers inform us that Disk 3 contains only the network administration tools. Ed.*]

Documentation

The *NVC* documentation contained voluminous amounts of information about the product. It comprised two manuals – 'Installing and Getting Started' (44 pages) and 'User's Guide' (150 pages). The printed documentation is really very good. It is clearly written, thoroughly indexed, and easy to read – one of the best that I have come across. A single, A5, 80-page 'Administrators Guide' was also provided, but this deals mainly with network issues which are not covered in this review.

The User's Guide contains a superb explanation of how *Windows 95* commences operation when a PC is booted. Included is a description of why a DOS virus going memory-resident is not as severe a problem with *Windows 95* as it was with previous versions of *Windows*.

Under *Windows 95*, all DOS sessions are virtual – they each have their own chunk of memory. Therefore closing the DOS box will also terminate the memory-resident part of the virus. The manual states, quite correctly, that the main focus should be on the damage that memory-resident viruses might do whilst a DOS box remains open.

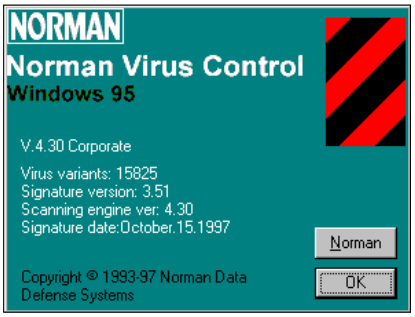
Another very well-written part of the User's Guide is the description of how the *NVC* behaviour blocker is implemented as a *Windows 95* 'virtual device driver' (VxD). I think *Microsoft* would benefit here – I can understand this text, but *Microsoft's* confusing prose is often beyond me. The *Norman Virus Control* documentation is the exact opposite – clear, cogent, descriptive.

A gripe I have with the manual is the claim 'Behaviour blocking is a relatively new technique in the fight against viruses'. Well, I hate to be picky, but actually it is not. The very first anti-virus products used pattern recognition and checksumming techniques. Behaviour blockers followed within just a few months, but they fell out of favour (for reasons that are explained below), and in recent years I have reviewed very few products that incorporate the technique. However, behaviour blockers do seem to be making something of a comeback. My New Year's prediction for 1998 is that they will die away just as quickly as they did first time round. We shall see.

Component Functionality

The documentation explains that *NVC* is split into several cooperating components – a standalone scanner, a memory-resident program that detects and/or removes macro viruses, a memory-resident program that acts as 'bait' (their word) for file viruses, and a memory-resident behaviour blocker. The behaviour blocker must be disabled 'before you install new applications'. A likely problem here is that nobody will remember to do this, and I bet the phrase is included in the manual so that when things go terribly awry the developer cannot be blamed.

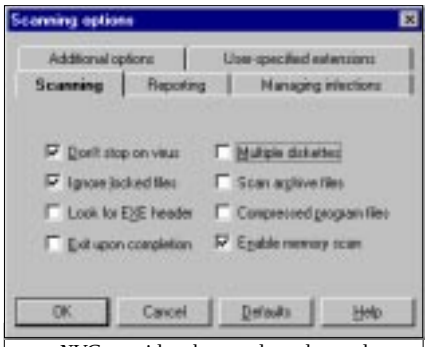
The manual states that the behaviour blocker is 'the key module'. I was fooled by this for a while – it was difficult to understand how anything other than the main scanner could be the 'key module'. It eventually dawned on me that the manual was referring to the facility to enable/disable various *NVC* components from the behaviour blocker icon in the system tray.



Scanning

The version of *Norman Virus Control* provided for review claimed knowledge of 15825 viruses. I tested its detection capabilities against the *VB* test-sets (see below) stored on CD-ROM. To say that I was astounded by the results would be to underestimate the thought processes I had to go through to come to the following conclusions. Read on…

The *NVC* scanner indicated detection of only 418 of the 549 samples contained in the In the Wild File test-set, and given its previously excellent reputation for detecting viruses, warning bells started to ring. The on-access macro scanner popped up to say that it had detected macro viruses, and the standalone scanner's report file also indicated that many files on the CD-ROM could not be accessed (see later for explanation). Close examination of the report file showed that all the samples from the In the Wild File test-set had either been detected as infected, or could not be opened. All this was most perplexing.



NVC provides the usual on-demand configuration options.

This result contrasted starkly with the 762 out of a possible 774 viruses (98.4%) that *NVC* detected in the Standard test-set. Remember that many if not most scanners have problems with the Standard test-set!

When the Macro test-set was scanned, I was at first totally flummoxed – the *NVC* scanner detected precisely none. This odd result was coupled with the fact that the memory-resident scanner popped up and warned that it had detected a macro-infected file. After much thought, several phone calls, and a bit of guessing, things became clearer.

The *NVC* standalone scanner knows whether the memory-resident scanner (which detects macro viruses) is present. If it *is*, then it leaves macro virus detection to the on-access component and switches macro virus detection off within the scanner. It is noticeable that the manual hints at this when it states that the *NVC* scanner is now supplied with two virus definition files – one for macro viruses, and one for file viruses. This means that the standalone scanner performs its tasks quicker, which is no bad thing. I tested this by disabling the memory-resident macro virus scanner, and sure enough the standalone scanner now detected 712 out of 716 macro viruses (99.4%). It only missed the four samples of Robocop – an *Excel* macro virus.

Were I to create a CD-ROM, or a floppy disk, and scan it for viruses, then it may well be stuffed full of macro viruses. If I was being particularly thoughtless, ignored the onscreen Cat's Claw warning and just read the report file, then I might think that the scanner report was correct and that the CD-ROM was not infected. I feel that some warning about this 'feature' is necessary. I certainly could not find it in the documentation, and I had a very good dig indeed in the entire scanning section.

Note that I am not really complaining about how well *NVC* detects viruses, but about how it tells you what it is going to do, what it has found, and what it has done.

Norman Virus Control's scanner scored a perfect 100% against the 91 viruses in *VB's* In the Wild Boot test-set. What more needs to be said?

The Polymorphic test-set contained 13,000 viruses (500 samples of 26 viruses), and the *NVC* standalone scanner detected all of them. 100%. This is a better result than most of *NVC's* competitors.

When I tested *NVC* against the *VB* Clean test-set (5500 executable files, held on CD-ROM, all of which have been copied from well-known software products, none of which are virus-infected), it did not find any virus infections. This result was the same with or without the memory-resident macro virus scanner enabled.

Speed

Using the default settings, *Norman Virus Control* scanned the C: drive of my test PC in 38.3 seconds. This was reduced somewhat (28.2 seconds) by removing the memory scan, and further improved to 27.3 seconds by disabling all the logging options. In comparison, the DOS version of *Dr. Solomon's Anti-Virus Toolkit* took 43 seconds, and the DOS version of *Sophos SWEEP* 42 seconds, to perform the same scan. When I reviewed a previous version of *NVC*, its scanning speed was inferior to competitor products, but now it appears to be one of the faster scanners around.

It is possible to slow down the scan, either slightly – scanning all files increased the scan time to 50.3 seconds, or dramatically – checking inside compressed files pushed it up to 2 minutes 19 seconds. Activating both these options simultaneously made the scan time 2 minutes 39 seconds. Scanning inside compressed files always slows things down, but *NVC's* scanner does seem more affected than most by having a scan time that varies by almost a factor of six depending on which options are activated at any particular time. Choose scanner settings with care.

Memory-resident Scanning

The memory-resident scanner provided with *NVC* is called Cat's Claw. This would be a strong contender in any contest for the silliest software name, but I suppose at least it is memorable. It only checks for macro viruses, and the version provided for review stated that it had knowledge of 1644 'variants'. Cat's Claw can be tailored in various ways to remove macro viruses from infected document files, all of which is eminently well explained, but many of the options rely on you having to take some action. The reality is that most people do not know what to do (apart from panic!) when faced with a message alerting them to a virus.

An option is also provided to 'certify' macros. In other words, code is added which allows Cat's Claw to detect if any change has been made to the macro. This is a good idea, and will work well within a large organization, but it is really something that *Microsoft* should have introduced so that everybody can use it.

Cat's Claw configuration is straightforward.

Cat's Claw proved to be very efficient at spotting macro viruses, and preventing access to infected files. Indeed, my earlier 'problems' with the *NVC* scanner stemmed from the fact that Cat's Claw denied access to all the macro-infected samples in the ItW File test-set. Similarly, if I attempted to copy a macro-infected file from the CD-ROM to the hard disk, the action was interrupted by Cat's Claw, a warning message appeared, and the copying was terminated.

Cat's Claw has an internal limit of about 24 warning messages, and gives up notifying you about viruses when this number of messages is awaiting confirmation. This point is not documented, and may fool those who find themselves on a badly infected PC. It fooled me for a while.

Remember that only macro viruses are detected by the memory-resident scanner. I could copy the Standard and Polymorphic test-sets (both macro virus-free) with impunity. However, when I tried to copy the In The Wild File test-set, the copy terminated when the first macro virus was detected, and the usual Cat's Claw warning messages appeared, awaiting user confirmation.

Behaviour Blocker

My problems with behaviour-blocking software are always the same – how do you know whether it is doing anything, how do you test such software, and why are the software's actions described so vaguely in the manual? *NVC* is no exception. The documentation states that the 'Smart Behaviour Blocker… monitors activity and intercepts virus-like behaviour'. Now this sounds good, even laudable, but what does it actually mean? It is impossible to arrive at an unambiguous definition of 'virus-like behaviour', but the *NVC* manual does attempt it. In fact, it provides more technical details than most similar products about what this behaviour blocker actually does, including a brave attempt at an explanation of how 'statistical analysis' is used to prevent desired actions being blocked. After reading all this, I am still left with the conclusion that fine phrases are being bandied around stating that it protects, detects and removes known and unknown file viruses, boot viruses… (you get the picture), but real definitions are being fudged. For instance, what type of statistical analysis is used? What happens with software that frequently updates its own executable files? I could go on.

None of these criticisms are unique to the *NVC* behaviour blocker, which is better than most. It provides several options whereby its action can be tailored, and (perhaps more importantly) it is easy to unload. All such products suffer because they fall between two stools: monitor too closely and the false alarm rate shoots up (which causes chaos!), monitor too lightly and most viruses escape detection (which may cause chaos!).

The Rest

Norman Virus Control includes a program called 'Canary' that acts as bait for viruses; i.e. it detects whenever it has been infected and informs you. In my last *NVC* review, I attempted to gauge the success of this ploy. My failure to achieve very much, despite literally days of effort, still scars my memory (see *VB*, May 1994, p.17). I did not repeat the experience this time round – life is too short.

NVC also includes information about the viruses it knows about, and a comprehensive scheduler. These two features appear to be very common, almost mandatory, with modern anti-virus packages, and both work well here.

Conclusion

The grandiose claim made at the start of this review is very close to being true – *Norman Virus Control* only missed four samples of a single *Excel* virus and it detected all the other macro viruses. However, some of the ways in which *NVC* operates are, to put it mildly, quirky. I am not saying that the mode of operation is wrong or inferior, it just does things in ways that are not initially clear. Once this is realized, *NVC* works very well, is very capable of detecting viruses (polymorphic detection is outstanding at 100%), and it scans quickly. It should prove to be a good buy.

Technical Details

Product: *Norman Virus Control v4.30* for *Windows 95.*

Developer: *Norman Data Defense Systems* AS, Strandveien 37, Lysaker, Norway, Tel: +47 6758 9930, Fax: +47 6758 9940, email: norman@norman.no, WWW http://www.norman.no/.

Availability: The manual states that 'Norman Virus Control can be installed on any machine with the appropriate operating system, it will however occupy a small portion of your hard disk which must be available'. The sharp-eyed reader will have noticed that this statement is completely bereft of any technical detail whatsoever. The README file lists the System Requirements for operating under *NT*, but says nothing on this subject for *Windows 95*.

Version evaluated: 4.30a Corporate.

Serial number: None visible.

Price: Pricing varies, depending on the number of licences and conditions. Contact your local distributor for details.

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

Test-sets: See *VB*, September 1997, p.16.

SUBSCRIPTION RATES

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

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

Editorial enquiries, subscription enquiries, orders and payments:

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

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

US subscriptions only:

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

Tel (781) 9377768, Fax (781) 9320251

END NOTES AND NEWS

After two successful exhibitions in the UK, **Infosecurity Asia 1998** will take place at the **Singapore International Convention and Exhibition Centre from 25–27 June 1998**. The event encompasses every aspect of IT security within a business environment, including anti-virus issues. For more information and a business reply coupon, contact Karen Binwani or Rose Zama at Reed Exhibitions Pte Ltd in Singapore; Tel +65 434 3663/3698, or fax +65 334 4119.

***Integralis* announces the release of *MultiPlatform CONTROL-SA* from *EagleEye Control Software*.** Aimed at organizations that use a number of different computer systems, the software centralizes security control across *Windows*, *OS/2*, and *Novell* operating systems in addition to covering *IBM*, *Digital* and UNIX platforms. Features include complete password synchronization, centralized alert functionality and real-time tracking/control of information. For details of prices, email info@integralis.com.

The new *Disknet Macro Interceptor* from *Reflex Magnetics Ltd* can be used as a standalone solution to macro virus threats or as part of the *Reflex Disknet Data Security Suite*. It requires a 486 PC running *Windows 95*, with a minimum 2 MB of free hard disk space and 16 MB RAM, and costs £19 +VAT per user for up to ten users. Contact Phillip Benge; Tel +44 171 3726666, or email phillip.benge@reflex-magnetics.co.uk, for details.

***Network Associates* has released *GroupShield* and *GroupScan* for *Microsoft Exchange Server v5.5*.** This dual-defence system, which also supports *Exchange* v4.0 and v5.0, incorporates both anti-virus and data security capabilities. *Network Associates* (formerly *McAfee*) claims that its Hunter technology, incorporated in these products, assists in locating new macro, boot and file viruses. For further details, contact the UK marketing manager Caroline Kuipers; Tel +44 1344 304730, email caroline_kuipers@cc.mcafee.com, or visit their Web site; http://www.mcafee.com/.

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

Trend Micro's InterScan VirusWall v2.5* for *NT, which monitors Internet traffic performance at the same time as blocking Java and ActiveX code, is to be distributed by *Peapod Internet*. The new release version also adds real-time cleaning of infected HTTP and FTP traffic, and is year 2000 compliant. It costs £1295 for 50 users. Contact Chris Durnan for details; Tel +44 181 6069924 or email chrisd@peapod.co.uk.

***Network Systems & Applications Management '98* will be held from 28–30 April 1998, at London's Olympia.** The event is the result of the amalgamation of three major IT exhibitions: *Infosecurity* has joined forces with *Customer Service & Support '98* and *Network, Systems & Applications Management '98*. More details, and contacts for all three subsidiary events, can be found on the World Wide Web at http://www.infosec.co.uk/.

***Network Associates* has announced *WebShieldX*,** which it describes as the first family of products to offer complete anti-virus protection, and filtering of hostile applets and email content in a single solution. At the same time, as the result of an alliance between *Network Associates* and *Trusted Information Systems*, *WebShieldX* is to be resold with the *TIS Gauntlet* family of network firewall security solutions. For more details, contact Caroline Kuipers (see above).

The industry-wide IT security alliance, **OPSEC, has been bolstered with the release of *MIMEsweeper for FireWall-1***. *Check Point's* Content Vectoring Protocol (CVP) acts as the communications channel through which *FireWall-1* can pass SMTP, FTP and HTTP file transfers to *MIMEsweeper* for disassembly and validation. *MIMEsweeper for FireWall*-1 operates either on the same machine as *FireWall-1* or on a remote machine and will run on *Windows NT 4.0*. Contact Sue Trussler; Tel +44 118 9306060, or visit the Integralis Web site; http://www.mimesweeper.integralis.com/.

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