ISSN 0956-9979 MARCH 1998

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

IN THIS ISSUE:

• **N-Tried N-Tested:** Several new viruses In the Wild and the old boot virus scanning problems contributed to just one vendor attaining a VB 100% award. This month's *NT* comparative starts on p.10.

• **Czech it out:** Pavel Baudis shows how Slovakia has become a 'real virus empire' compared to its neighbour. Read his report from the former Czechoslovakia, on p.8.

• **Where in the World?** The News Page contains long-awaited information about the dates and location of this year's *Virus Bulletin* conference, on p.3.

CONTENTS

EDITORIAL

Trojan Sciamachy

Recently, there has been a flurry over a new, not released to the wild, 'email virus'. A well-meaning press release didn't quite get the right message clear enough, the result being dozens of concerned citizens posting to Usenet and mailing lists about this new 'real email virus'. The point missed in this is that a virus just using email as a file-transfer mechanism is not an 'email virus'.

The 'you can get a virus just by opening an email message' myth may well have been strengthened. Probably not bad news for the shysters selling email scanners as *the* solution to your virus problem, but also, I suspect, not the intended outcome of the press release. I guess it may be coincidental, but we seem to have seen a huge resurgence in the 'Join the Crew', 'Return to Sender', etc mass email hoax messages since that fateful press release. Interestingly, press releases and 'email-borne nasties' of another sort have been on my mind for some time. I pointed out at VB'97 that you should be wary of the hypesters with vested interests in convincing you (or someone) that email-distributed Trojan Horses were the 'next big worry'.

" no software can protect you from Trojans "

Well, those people are still out there and they have a product to help protect you against this new threat. Sales must not be going well – they have recently been promoting this as a major concern.

At the *VB* office we recently received a press release from a major anti-virus vendor listing the ten most prevalent viruses it had had reported in the previous month (it must have been a slow day in their marketing department that day). Cap, Concept, AntiEXE, Form… you get the picture – *nearly* as riveting a read as a year's back issues of the *VB* Prevalence Tables!

As we seldom have slow days in the *VB* office – at least none that slow – it was soon arcing toward the circular file. But wait… what was that lurking down the bottom of the list, rated tenth-equal with, but nearly overshadowed by, Laroux? '& various password stealing trojans' Tell me more!

And they did. A 'senior technology consultant' had been shaken down and dusted off to inform the awaiting hordes of the press of this terrible new scourge. Let's not beat about the bush here. We *are* talking about *AOL* password-stealing Trojans. There are, of course others, but the only ones of any consequence recently, are these. *AOL* does not officially admit they are a problem. After all, when you are 'the best', you don't have problems, right? – just ask *Microsoft*!

The press release politely skirts the issue that these are mainly only of concern to *AOL* users. Worse however, it ignores the issue of whether anti-virus software can really afford any significant degree of *protection* against this menace, 'growing quickly at a rate of around one to three each day'.

In case you haven't guessed, I don't believe that any *software* can protect you from Trojans. They are, unlike viruses, not self-spreading. Trojan Horse events tend to be point occurrences – a Trojan appears (often in highly localized settings), draws attention to itself and is never seen again (apart from in the collections of people who might otherwise find trainspotting a worthwhile pastime).

Advocating scanning as 'protection' against Trojans fosters an inaccurate image of what the anti-virus industry can do for its users. Just as you cannot definitively determine whether an aribitrary file is a virus, you cannot tell whether it is a Trojan. As Trojans don't tend to 'last', detecting them, whilst not completely pointless, is much less valuable than adding detection of viruses to a scanner. Anti-virus users seem to accept that new viruses might not be (properly) dealt with when first they arise. The flip side is that any virus incident they have is quite unlikely to involve a new virus.

However, the balance is quite different with Trojans. Setting itself, and by association the rest of the industry, up as 'the Trojan protectors', this developer is courting trouble. It will be pointed out that a few Trojans have reappeared repetitively in Usenet postings and many new *AOL* password stealers can be found heuristically. True, and detecting these could be a worthwhile addition to a scanner. However, using these historical oddities to project a profitable future in bolting Trojan detection onto anti-virus software is folly. Your users should simply not run untrusted software!

NEWS

VB'98

This year's *Virus Bulletin* conference is to be held at the Hilton Park Hotel, Munich, in Germany. The two-day conference will again present corporate and technical streams, and runs from Thursday 22 to Friday 23 October 1998. A welcome drinks reception is scheduled for Wednesday 21 October. Contact our Conference Manager for details; Tel +44 1235 555139, fax +44 1235 531889, or email alie@virusbtn.com.

VB'98 coincides with the second largest IT show in Europe. For the first time, *Systems'98* will take place in the purpose-built Munich Trade Fair Centre; running for the week commencing 19 October 1998. More information about *Systems'98* can be found at http://www.systems.de/.

Errata

Virus Bulletin apologizes to *IBM* and *iRiS Software*. Following a lengthy investigation, we have found some errors in the In the Wild Boot test results published in the January *Windows 95* comparative review. We reported that both products missed two samples from that test-set – Michelangelo and MISiS.

On re-testing these products on the original test machine and several others, *IBM AntiVirus* and *iRiS AntiVirus* always detected these viruses. Other products that also failed to detect these viruses in the original test still failed to detect them in the re-testing. Efforts to reproduce the conditions that led to the original testing failure have been unsuccessful. As a precautionary measure *Virus Bulletin* will not use the computer that gave rise to the suspect January results in future boot sector testing.

Unfortunately, this error means that *IBM AntiVirus for Windows 95* was not recognized with the VB 100% award it deserved. *Virus Bulletin* would like to thank the technical staff at *IBM* for their assistance in attempting to locate the source of this error. Subsequent reprints of the January test results will contain the correct scores.

Czech-or-Slovakian?

Our apologies are also due to two anti-virus companies based in the former Czechoslovakia which participated in February's DOS comparative review. In last month's issue, we referred to the anti-virus company *Grisoft* as Slovakian, and to Slovakian *ESET* as Czech.

To clarify – *Grisoft*, the developers of *AVG* are based in the Czech Republic, while *ESET*, the company which produces *NOD-iCE* operates out of Slovakia. Had we already read Pavel Baudis' article published this month (see p.8) this *faux pas* would have been avoided.

Prevalence Table – January 1998

Virus	Type	Incidents	Reports
CAP	Macro	97	20.7%
Concept	Macro	29	6.2%
Form	Boot	29	6.2%
AntiEXE	Boot	27	5.8%
Parity_Boot	Boot	22	4.7%
Monkey	Boot	17	3.6%
Ripper	Boot	17	3.6%
Laroux	Macro	16	3.4%
Npad	Macro	15	3.2%
Dodgy	Boot	13	2.8%
NYB	Boot	13	2.8%
Wazzu	Macro	10	2.1%
AntiCMOS	Boot	8	1.7%
Temple	Macro	8	1.7%
DelCMOS	Boot	7	1.5%
Appder	Macro	5	1.1%
Goldfish	Macro	5	1.1%
Imposter	Macro	5	1.1%
Junkie	Multipartite	5	1.1%
Maverick.1536	File	5	1.1%
PayCheck	Macro	5	1.1%
Schumann	Macro	5	1.1%
WelcomB	Boot	5	1.1%
ABCD	Boot	4	0.9%
Galicia.800	Multipartite	4	0.9%
Johnny	Macro	4	0.9%
NiceDay	Macro	4	0.9%
Sampo	Boot	4	0.9%
ShowOff	Macro	4	0.9%
DZT	Macro	3	0.6%
Exebug	Multipartite	3	0.6%
Lunch	Macro	3	0.6%
Natas	Multipartite	3	0.6%
Quandary	Boot	3	0.6%
V-Sign	Boot	3	0.6%
Others [1]		59	12.6%
Total		469	100%

[1] Comprising two reports each of: ABC, Bleah, Eco, GoodNight, Kompu, Moloch, Mtf, Razer, She_Has and Swlabs; and single reports of: Angelina, Bandung, Barrotes, Bonus, Cascade, Colors, CountTen, Delwin, Demon, Dinamo, Dub, Edwin, Flip, Helper, Int12, Jerusalem.Zerotime.Australian.A, Jimi, Kampana, MDMA, Muck, Munch, NF, NoInt, NOP, Oxana, Pieck, Rapi, Spanska.4250, Stealth_Boot, Stoned, Tentacle, Tentacle_II, Tequila, TPVO, Tubo, Twno, Uruguay, V2P6 and V-947.

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 February 1998. Each entry consists of the virus name, its aliases (if any) and the virus type. This is followed by a short description (if available) and a 24-byte hexadecimal search pattern to detect the presence of the virus with a disk utility or a dedicated scanner which contains a user-updatable pattern library.

Type Codes

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

Alia.1023

ER: A polymorphic, encrypted, 1023-byte appender containing the text 'ALIA'. All infected files have the byte 43h ('C') at offset 0001Ah. The following template only detects the virus in memory.

```
Alia.1023           2EA1 9000 3D4D 5A74 03E9 1002 2EA0 AA00 3C43 7503 E905 02B0
```

AntiWin95

DMR: A one-sector boot sector virus infecting hard disk MBRs and floppy DOS boot sectors. It does not save the original boot sectors. The system always boots from an active hard disk partition. It contains the text 'AntiWin95' at offset 003Eh – the first two characters are used in self-recognition.

```
AntiWin95           B801 008E D880 3E72 043C 7448 FABE 0304 AD48 4E4E 8904 FBB1
```

Coup.2260

MCER: A multi-partite, stealth, encrypted, 2260-byte appender containing the text 'Coup De Main : Please Say She Don't Annoy Me !!!'. When infecting a hard disk, the virus stores its code in cylinder 0, head 0, sectors 3, 4, 5, 6, 7 and the original MBR in cylinder 0, head 0, sector 8. After a machine boots from an infected disk ten times, the virus displays its message – after fifteen boots, it disinfects itself and restores the original MBR. Both patterns can be used for memory detection.

```
Coup.2260 (MBRs)    BA80 00FA 8306 8600 0483 2E13 0404 B800 9F8E C050 FBB8 0602
Coup.2260 (files)   2E28 042E 8034 8046 2EFE 0629 0459 E2D1 2E80 3E2A 0401 740D
```

Energy

MDR: A boot sector virus infecting hard disk MBRs and floppy DOS Boot Sectors. Two sectors long, it stores the original MBR and its second sector on hard disks in cylinder 0, head 0, sectors 14 and 15. On floppies, the original DBS and the virus' second sector are stored in cylinder 0, head 1, sectors 14 and 15. The virus contains the texts 'Tel: (401) 778.08.48', 'Virus detected!(c) 1997 »-» ¡Energy!', 'Boot anti-virus! For details & upgrades call :0123456789ABCDEF' and 'INT 13h points to => F000:97F4'.

```
Energy              2681 BFE9 00AF AE74 3F80 FC03 741F E80B 01B0 01E8 1B01 7229
```

Ermua

MDR: A family of boot sector viruses infecting hard disk MBRs and floppy DOS Boot Sectors. Variant A contains the text 'M.A.Blanco Garrido-Ermua[King Lizard]', variant B '{♥Lady Di♥}' and '[(C) King Lizard]', variant C '{Lady Di}' and '[King Lizard]'. The virus stores the original MBR in cylinder 0, head 0, sector 2. Variant A infects only 1.44 MB diskettes and stores the original DBS in cylinder 79, head 1, sector 18. Variants B and C store the original DBS in cylinder 0, head 1, sector 3 (360 KB) or sector 14 (720 KB, 1.2 MB) or sector 15 (others).

```
Ermua.A             04FF 7703 5848 508F 4703 6BC0 4050 0787 064E 0050 8F06 4D7D
Ermua.B             04FF 7703 5848 508F 4703 6BC0 4050 0787 064E 0050 8F06 617D
Ermua.C             04FF 7703 5848 508F 4703 6BC0 4050 0787 064E 0050 8F06 6C7D
```

Exeheader.406

ER: A stealth, 406-byte virus inserting its code into the headers of EXE files. It requires the presence of HIMEM.SYS and contains the text '> Joan v1.2 by KiKo NoMo of T.N.T. Taipei/Taiwan 1995/08 <'.

```
Exeheader.406       354D 5A74 1126 803F EB75 4426 817F 5CB4 0D74 2EE9 3900 2683
```

Exeheader.448

ER: A 453-byte virus inserting its code into the headers of EXE files. The virus contains the text 'Work448(Bob)'. Infected files have the word 0000h at offset 0008h (size of actual header).

```
Exeheader.448       B9C0 010E 1FBA 0600 B440 CD78 33D2 3BEA 740F 8BCD 03C9 03CD
```

Fairground.813

ER: An encrypted, 813-byte appender containing the texts 'F:\LoGiN\LoGiN.eXe', 'TB', 'SC', 'KR', 'WI', 'F-' and 'FAIRGROUND (c) BlackFlash!'. It only replicates from May to December..

```
Fairground.813      81C3 3E00 B9EC 028A 07E8 0800 8807 43E2 F61F EB12 5053 51B8
```

Flag

DR: A one-sector boot virus infecting both hard disk and floppy DOS Boot Sectors. The original DBS is stored in cylinder 0, head 0, sector 7 (hard disks) and cylinder 0, head 1, sector 3 (floppies).

```
Flag                2E81 3E40 04B8 0074 31B8 0103 B907 00BA 8000 CD13 FC0E 1FBE
```

Glitter.2207

CN: An encrypted, 2207-byte appender infecting COM and SYS files (device drivers). It contains the text '♥ Glitter ver 1.0 , Coded by Siddharth.♥ SID IS IN YOUR RAM CHIPS ♥ ♥ Greetings From Siddharth Bombay-92♥' and 'CHKL*.*'.

```
Glitter.2207        83EE 050E 07C6 441D 908A 5420 B995 04BB 2300 3 010 43E2 FBC3
```

Hammer.2272

CER: A 2272-byte virus containing the plain-text message 'Fatal error A3041' and the encrypted texts 'EXEexeCOMcomMASMmasmTASMtasmFANTfantWEBwebAIDSaidsANTIantiSCANscanCOMMcomm*.*', 'Hammer-96;OWY + VRN-1600 - BASE;' and 'ANTI-DBE;2222,213 SLAYER...OWY 1.00...'.

```
Hammer.2272          E800 0058 1E2D 0400 50B4 D5CD 213D 5634 7503 E9B8 005F 5706
```

Hoodlum.777

CN: A double encrypted, appending, 777-byte, direct infector containing the texts 'HOODLUM VIRUS SAYZ! -> FUCK ALL YA HOES!!\', '*.com' and 'command.com'.

```
Hoodlum.777          80BE 2001 B974 4FB9 0C04 8DBE 2001 2E80 3501 47E2 F9B8 0D05
```

House.391

CN: A polymorphic, appending, 391-byte, slow, direct infector infecting two files at a time. It contains the text '((BUBBLE-HOUSE))'. Infected files have their time-stamps set to two seconds. The virus implements a short, but effective, table-driven polymorphic encryption mechanism with a number of appended bytes varying between 391 and 397. It is impossible to select a simple virus template, however, the infected files always end with the sequence 47h 4Dh 75h F?h C3h.

Insert.271

CR: An encrypted, 271-byte prepender infecting on File Create (Int 21h AH=3Ch or AH=5Bh). It contains the text '[Insert] [Darkman/VLAD]'. It is impossible to select a template longer than 12 bytes.

```
Insert.271           B97E 0081 35?? ??47 47E2 F8C3
```

Kate.585

CR: An appending, 585-byte virus containing the text ' KATE 1996 - (C) ORIEL software company '. Infected files have the word 4B4Dh ('MK') at the end of their code.

```
Kate.585             9C3D 4D99 7504 B04B 9DCF 80FC 4B74 0580 FC3D 75E6 60FC E800;
```

Madman.1663

ER: An encrypted, 1663-byte appender containing the text 'Nothing can save you here, friend - you're in my world now!', '@ECHO I'm watching you!' and 'MadMan'. The first message is displayed when Alt+Ctrl+Del keys are pressed, the second is appended to BAT files. Infected files have the word 4D4Dh ('MM') at offset 0004h from the end.

```
Madman.1663          8CC8 2D10 00FA 8ED0 B9FF 0231 ED81 B664 02E7 F345 4590 9090
```

Mainman.407

CN: An appending, 407-byte direct infector containing the text '*.com'. On Sundays, the virus does not replicate but displays the word 'VIRUS'.

```
Mainman.407          B640 B997 018A E68D 9603 01CD 21B4 3ECD 21B4 3B8D 968D
```

Moskau.800

CN: An encrypted, 800-byte appender containing the text '<MOSKAU98>Stas'. Infected files start with the word DE03h (ADD BX, SI).

```
Moskau.800           0A8B F581 C659 018C C8CD 013E C686 C400 568B C505 C602 FFE0
```

Mrodehna.5154

CER: A polymorphic, stealth, encrypted 5154-byte virus containing the texts 'Hello Mr. Odehnal !', 'GRISOFT(c) SOFTWARE 1989,96', 'BE CAREFUL !', 'CMOS-DEAD: DATA DESTROYED !', 'V', 'F-', 'TB', 'SYS', 'SCAN', 'CLEAN', 'WIN', 'GUARD', '286', '386', 'CHK' and 'EXECOM03/28/96'. The payload overwrites the MBR of the first physical hard disk. The following template only detects the virus in memory.

```
Mrodehna.5154        3DCD 4D75 05B8 08CD 9DCF 80FC 4C75 072E C606 3D0F 0090 2E80
```

Piz.1176

CER: An encrypted, 1176-byte appender containing the text 'o*p*p*o*u*'*'. Infected files start with the word E94Dh.

```
Piz.1176             3DAF FA75 12B8 B0B0 CF2E 803E 7001 E974 F82E C606 7001 E9F7
```

Small_comp.155

PN: A companion 155-byte direct infector containing the text '*.exe'. The virus creates up to four hidden, read only, system identical COM files at one go.

```
Small_comp.155       B440 B19B 32D2 CD21 B40E 0D0A 30CD 21B4 4A33 F68D 5C1D CD21
```

SillyRC.482

CR: A 482-byte appender similar to SillyRC.212 and SillyRC.476 (see *VB*, September 1995, p.5). It contains the same texts 'Subconsious virus - Conzouler/IR 1995.', 'Mina tankarér det sista som ni tar...' and 'LOVE LOVE LOVE LOVE LOVE LOVE LOVE LOVE'. Infected files have the byte EAh at the end of the code. It can be detected using the same template published for the 476-byte variant.

```
SillyRC.476/482      4F56 453D 7742 7501 CF3D 004B 756C 5053 5152 1EB8 823D CD21
```

Solar.123

ER: A 123-byte appender infecting files on execution of the Write function (AH=40h, INT 21h). Infected files start with the signature 'ZM'.

```
Solar.123            80FC 4075 4D8B F2AD 3D4D 5A75 45AD 3D85 0173 3F8B E9C1 ED09
```

TimberWolf.546

CN: A prepending, 546-byte direct infector, containing the texts 'Timber Wolf by Quantum / VLAD', 'ATH..' and '*.com'.

```
TimberWolf.546       B922 02BA CEFA CD21 E825 00B9 2202 BACE FAE8 2C00 5AE8 0C00
```

Unashamed.C

MDR: A boot sector virus containing the encrypted text 'I'm the great UN, say, the Unashamed Naked! Yeah! of course, I'm the pride of yo nud(ll)ity! I'm here to nakedly spread my HELPS, say, my AIDS along with my UNashamed & AmeriKindily famous dinocracy, yo girl♥ & pearl$ in my heart! Uh! I ♥ this game! Pray fo peace guys, while I seize, strip, kis♥ & $queeze! You'd enjoy the scene & hold yo hate, I've no shame, once I'm spreading AIDS, for(the)sake (of)yo peace! Sure! In Songola, Moznia, Amalia, Bozambique,... my stripsqueeze's going on, UNashamed & NAKEDly! UN, watch yoself!... Black Synapse advises!'

```
Unashamed.C          BE00 7C8B E68B FBB9 0300 298C 1388 8B84 1388 D0E1 D3E0 B900
```

VIRUS ANALYSIS

Tales from the Cryptor

Frédéric Perriot
IBM

Cryptor is a family of very basic, direct action file infectors. Its members do have a fairly complex polymorphic engine and some anti-emulator features which make them interesting. This analysis focuses on the smallest member of the family of polymorphics composed of Cryptor.2169, Cryptor.2582 and Cryptor.3612 (versions 1.0, 1.5 and 2.0, according to their author 'Night Spirit').

Cryptor.2169 causes problems for several emulators because the polymorphic heads it generates can contain instructions that behave slightly differently from one processor to another. Given 'compatibility' with the PC, Cryptor.2169's body will be decrypted, restoring the first four bytes to the host, carrying out the infection and finally executing. There is no payload in this virus.

The Replication Code

Cryptor is a direct action, parasitic infector. It will infect every COM file in the current directory with a length between 1000 and 60,000 bytes. The fourth byte is compared to 24h ('$'). On a match, the file is closed and passed over. Otherwise, the virus checks the file size, and if within the above bounds, calls the polymorphic engine to generate a new sample which is written at the end of the host. It continues by seeking back to the beginning, writing the jump and the marker, closing the file and using FindNext to find another victim, until it has tried all the files in the current directory.

The code dedicated to replication is only 181 bytes long and its error checking is minimal. No check is made for EXE files with COM extensions, nor for attributes. Read-only files are not infected. Infection changes the file's time and date and adds an average 2525 bytes. (In tests on 10,000 samples the standard deviation was 37 bytes.)

The Polymorphic Engine

The engine in Cryptor.2169 (or 'Universal Polymorphic Device v1.0' as the author calls it) can generate a large variety of instructions, which can be divided into five groups. Consecutive instructions are unrelated, making it obvious at first glance that the decryptor is full of garbage.

The first group is composed of nineteen, single-byte instructions. These mainly involve flag manipulations, segment override prefixes, packed and unpacked BCD adjust instructions, plus DEC, INC and XCHG with the accumulator of a random register (apart from SP, which the virus carefully avoids).

The second group contains twelve assignments, shift, arithmetic and logic instructions, NOT, NEG, MUL and IMUL, nine arithmetic and logic instructions with a random immediate value as second argument, and the two-byte versions of INC and DEC. These 'instructions' are really templates corresponding to opcode masks – opcodes plus random byte or word registers and variable arguments. The second group is also supposed to contain nine arithmetic and logic two-byte instructions, but due to a bug in the engine, these are never generated.

The third group consists of eight single-byte instructions including string instructions, LAHF and XLAT. The fourth contains ten assignments, arithmetic and logic instructions that may use any byte register in the destination argument, and indirect (either based or indexed) addressing without a displacement in the source argument.

The fifth and last group is composed not of opcodes but rather of atomic instruction groups forming Int 21h calls that contain a MOV AH,<byte> Int 21h. Where necessary, these may be framed by a PUSH ES and a POP ES. The functions are 0Bh (Get STDIN status), 19h (Get Current Drive), 2Ah (Get Date), 2Ch (Get Time), 30h (Get DOS Version), 4Dh (Get return code), 51h (Get PSP), 54h (Get Verify Setting), 62h (Get PSP), 2Fh (Get DTA), 34h (Get INDOS flag), 35h (Get Vector) and 52h (Get list of lists).

When it is called by the replication routine, the polymorphic engine proceeds as follows. It loads various tables which describe how many encryption methods to use, which register to use as the pointer and which to use as the counter in the decryption loop. Then it computes a checksum on a 'copyright' message, messing up the stack if it does not match – eventually leading to a crash in most cases. Next comes the polymorphic head generation, where the virus generates between 40 and 80 random instructions from any of the five groups described above. This code is absolutely useless. The 'useful' stage is where the registers are loaded and the body is decrypted. The virus generates this decryption and the inverse encryption in parallel. An important point to mention here is that the values of all the general use registers are used as the key in Cryptor's decryption loop (rather than just a single value as in simpler encrypted viruses).

A variable piece of code loads FFFFh into AX and either sets or resets the carry flag. This isolates the useless code and 'seeds' the processor state. None of the random instructions generated thereafter, using AX or the carry flag, will then yield a result dependent on an exterior factor – which is more than likely to vary from the time of the encryption to that of the decryption. Then comes code to load the seven-word registers (not SP) in random order, interspersed with random instructions from the first group

(DEC, INC, XCHG with AX excluded, since these might cause undefined parameters from the useless bit to influence the key generation).

At this point, the state of the processor is well-defined and the piece of code that follows in the decryptor head is designed to make it evolve in a deterministic way, independent of the program's environment. The particular piece of code after the register loading is composed of 40 to 80 instructions taken exclusively from the first and second groups, which guarantees that nothing outside the processor state influences the key. This key generation phase appears in both the decryption and encryption routines.

Finally, the decryption loop itself is generated (the inverse encryption loop being generated in parallel at another place in memory). It starts with code to load the counter (with LEA or MOV) and the pointer (with a variable CALL/POP relocator). There are three to sixteen encryption instructions, that can be anything from NEG, NOT, INC, ROL1, ADD, DEC, ROR1, SUB to XOR applied to the dereferenced pointer, using a random register as the second argument if one is required. There follows the pointer increment and counter decrement, once again variable, and the loop instruction (LOOP or JNZ). Pffff... Done with it!

After the engine has generated both the decryption and inverse encryption routine, it applies the encryption to the virus body, prepends the decryption routine, and returns the length of the new sample to the replication code, which can then write it to the host file.

Anti-emulator Features

Cryptor may have been designed to cause problems to emulators. Whether it was or not, it has caused some discussion amongst anti-virus developers. The virus' attempt to fool emulators into thinking that the decryptor code is just casual program code is obvious from its use of numerous Int 21h function calls (see the list above). This is not that much of a problem, because the return values from these functions are never used. As we saw earlier, these function calls appear only in the first, 'useless' part of the decryptor and are surrounded by completely unrelated code. Thus, an emulator treating them as no-ops will do fine. However, strict emulators may encounter problems in this first part, because it often contains instructions that access words across segment boundaries.

The real problem comes after that, while trying to emulate the key generation portion of the decryptor. This piece of code affects the register loading and contains random instructions from the first and second groups. Thus it can include BCD adjust and MUL/IMUL instructions. The behaviour of BCD adjust is partially determined by the value of the auxiliary carry flag (AF) which, after MUL or IMUL, is undefined. This, however, does not mean that it is unknown. For instance, on some processors, AF is unchanged after a MUL, on others it will be reset, and on yet others AF's state after a MUL depends on the input values. Thus, in order to obtain the same decryption key under emulation as at encryption time, the emulator would have to imitate exactly the processor of the machine on which the virus sample was generated. The emulator may have to mimic all processors' behaviours for each potential virus sample! This raises a performance problem which can be solved by selecting only those samples containing some instruction patterns for 'multi-emulation'.

A second problem is how to emulate the exact behaviour of a specific processor for a given, partially undocumented instruction like MUL. The 'one-table-per-processor' approach is simple but would very quickly become impractical. Finding the flag's equation for each processor is sometimes possible, but takes a long time. The commonest problem is that of the MUL/IMUL followed by BCD adjust preventing some 386/486-generated samples from decrypting correctly on Pentium or Pentium Pro CPUs (true for about 8% of replicants). Other problems involve TEST followed by BCD adjust and shift instructions. Documenting all these instructions is certainly tedious work and may become an impossible task as chips get more complex.

A different approach would simply note that a 'problem' flag was involved in the instruction to be emulated. Should it eventually be decided there is no virus, the emulator would 'rewind' to that point and the other flag state would be emulated.

Even if Cryptor.2169 makes emulation more difficult, it is still perfectly easy to detect based on the analysis of the decryption head. Moreover, it does not spread well and it generates a lot of V86-mode intendeds. This applies equally well to the other two Cryptors.

Cryptor.2169 is a true polymorphic virus, but observing its polymorphic heads reveals a constant architecture. This can be used for detection purposes, obviating any 'advantage' its author may have hoped to gain from its polymorphic convolutions. Seeing beyond its decryption layer in a reliable way involves tons of tricky processor details, but is, ultimately, unnecessary for the virus scanner. Fortunately, like the other Cryptors, it is a dumb direct infector and carries no payload. Next!

Cryptor

Aliases:	None known.
Variants:	Cryptor.2169, 2582 and 3612.
Type:	Direct action, parasitic, polymorphic COM infectors.
Self-recognition in Files:	24h ('$') at offset 04h.
Hex Pattern:	None possible.
Removal:	Under clean system conditions, identify and replace infected files.

FEATURE

Virus Czech

Pavel Baudis
Alwil Software

In the Beginning…

The former Czechoslovakia experienced its first computer virus, Vienna-648, at the same time as neighbouring countries in the spring of 1988. It took almost a year for others including Cascade.1701, Dark_Avenger.1800, Vacsina and Yankee_Doodle to be seen. Several variants of Yankee_Doodle appeared among the most widespread viruses over the next few years.

The so-called 'Velvet revolution' brought not only political change, but also extensive economic expansion. This was reflected in the increased use of computers (especially *IBM*-compatible PCs). The computer boom, coupled with the growth in international contacts both far and near, influenced the virus situation in Czechoslovakia significantly. In addition to the Yankee_Doodle family, PingPong, MusicBug, Green_Caterpillar.1575, Stoned and Michelangelo appeared at this time.

The first Czech virus was probably Yankee.Login, which recorded all the user names and passwords entered via the *NetWare* LOGIN.EXE utility. It was possible to misuse this information to access unauthorized networks. Semtex was the first virus created in Slovakia. Regrettably, the Czechoslovak media took part in the exaggerated campaign which forecast catastrophe and made Michelangelo the hit of 1992. Although the events of 6 March made a mockery of that prediction, there were painful data losses in some cases. The DIR_II virus also caused great excitement when it spread and later disappeared equally rapidly.

On the other hand, Civil_Defense.6672 achieved long-term success. It was much more successful in Czechoslovakia than in Russia, its country of origin. This quite long and complex virus contains many effects (Russian songs, political slogans and even poems, flashing keyboard lights and simulated keyboard errors). In many cases it was detected only because of its conflict with disk types in the CMOS memory on some computers. This virus infects the MBR on hard drives and EXE files on diskettes, spreading from one PC to another. It is interesting that a similar principle was used later in the Slovak virus One_Half. Other examples of local viruses include the Helloween family, the politically-focused Pojer, and nationalistic Slovakian viruses, 'Tiso a Murgas'.

On 1 January 1993, Czechoslovakia was divided into two individual states: the Czech Republic and Slovakia. Fortunately, the split was very calm and peaceful and both new states maintain common interests, close economic relations and many other contacts. The virus scene developed quite differently, however. While nothing really interesting happened in the Czech Republic apart from a few local, boring viruses, within a few years Slovakia became a real virus 'empire'.

In Slovakia

Slovak viruses include Dzino, Monte_Carlo, Explosion and the infamous One_Half (there are several variants, but those most widely spread are 3544 and 3577). One_Half appeared in the spring of 1994 and remained the most widespread virus in the Czech Republic and Slovakia for years. Undoubtedly, the fact that many foreign anti-virus products were unable to detect this virus for more than a year contributed to this situation. The virus is unpleasant mainly because it encrypts data on the hard drive – removing the virus outright can cause serious data loss.

Interestingly, one Slovak newspaper reprinted an IRC debate (about software piracy), in which Vyvojar (Developer), the author of One_Half, participated anonymously. Asked why he built data encryption into his creation, he replied that he did not want users to remove the virus but to share their computers with it. Then came Lion_King.3531, but it did not spread much, and another One_Half descendant, Explosion Level 3. Two new Slovak viruses appeared in 1996 – DarkParanoid (see *VB*, January 1998, p.8) and Tiny Mutation Compiler (there are two variants of TMC: Level 42 and Level 69).

DarkParanoid contains an interesting innovation. It is fully polymorphic in memory. The virus is encrypted in memory and is decrypted one instruction at a time. Encryption and decryption are done via Int 01h, but even this routine is polymorphic and it is created when the virus installs itself in memory. The principle behind the process is explained in the text, which reads 'ENGINE OF ETERNAL ENCRYPTION'. However, the virus operation itself is so complex and computer slowdown so visible that its spread is almost impossible.

The TMC virus is a memory-resident, parasitic COM and EXE infector of 4835 bytes. It infects on file opening and rename, and on program execution, setting files' seconds value to eight. It contains the following text:

```
TMC 1.0 by Ender from Slovakia
Welcome to the Tiny Mutation Compiler!
Dis is level 42.
Greetings to virus makers: Dark Avenger,
Vyvojar, Hell Angel
Personal greetings: K. K., Dark Punisher
```

Tiny Mutation Compiler's text reveals how this virus is unique. When active in memory, TMC is able to change its body by switching instructions, yet it still remains func-

tional. So it is polymorphic not only in files but also in memory. TMC's so-called 'compiler' creates a copy of the virus in memory modified from pseudo-code stored in the infected file. This pseudo-code is static but encrypted. Nowadays this virus is successfully spreading in the wild in the Czech Republic and especially in Slovakia. This is particularly true of the Level 69 variant.

Today Slovak virus authors are working on macro viruses too. Even in this field they seem to specialize in technical 'advances'. It all began with Slow (or SlovakDictator, see *VB*, August 1997, p.15) which marks the first attempt to create a polymorphic macro virus. However, its operation was too slow and so noticeable to users that it earned itself the name Slow.

The next attempt – a virus called UglyKid – was more sophisticated. The third Slovak macro virus was Navrhar (HZDS), which (like Anarchy.6093), infects both *Word* documents and *Windows 95* VxD drivers (see *VB*, November 1997, p.15). The texts in these macros (and attached files) are directed against the Slovak political party HZDS, or more directly against its leader, the Slovak Prime Minister Vladimir Meciar.

The electronic virus magazine, Asterix, was released in Slovakia last year. So far, only one issue exists, containing a short description of Dark_Paranoid, TMC, and Slow, in addition to the four-byte long Kyjacisko. Asterix magazine is also mentioned in a file attached to Navrhar, in which the next issue is announced.

In the Czech Republic

The simple boot virus J&M appeared in the Czech Republic in 1993. It tries to format track zero of the hard drive on 15 November. The media campaign invoked by one local anti-virus firm prior to that date resembled that of Michelangelo, but again, there was no apocalypse. Moreover, the damage caused by J&M could be repaired quite easily. J&M is still very widespread and every year reports of inaccessible disks are received in mid-November. Much more dangerous is Ripper (which, with fixed probability, swaps two words during disk write operations). It is also widespread. Tremor arrived shortly after Ripper, soon to be followed by Natas.4744, imported directly from Mexico.

Local Czech viruses include the Helloween family, several Pojer variants, Raptor variants, Vzpomen (Velvet), Vic, Czech Happy, Klepavka, Ebola, Pivrnec, several variants of CMOSDeath and also brand new viruses Pastika.2049 (December 1997) and Animals.2400 (January 1998).

The first macro virus appeared in the Czech Republic in September 1995. Of course, it was Concept. Most users and companies use the Czech version of *Word*, under which (due to localization) it is not possible for Concept and most other common macro viruses to spread. So Concept appeared mainly in organizations which cooperated with foreign (especially American) partners.

Apart from this, nothing important happened for almost two years, except for occasional reports of Date, MDMA and Npad. Last summer Bertik emerged. It had the potential to spread more widely because it works properly under both Czech and English versions of *Word*. However, there was no mass expansion such as that caused later by CAP. This virus caused a big epidemic here as in many other countries and was like a cold shower, with many users meeting a macro virus for the first time. Nowadays, CAP is the most widespread virus in the Czech Republic, but in the last six months Laroux (for *Excel 5/7*) has spread notably too.

The Situation Today

CAP.A leads the field, with Laroux quite far behind. J&M is the most prominent of the boot viruses, followed by Ripper, Form, AntiCMOS, WelcomB, Parity_Boot, Spirit and Angelina. File viruses are also relatively widespread, especially Pieck.4444, Pojer.4028, TMC (especially in Slovakia) and Helloween.1376. The Alfons.1344 and Burglar.1150 viruses have been distributed on CDs accompanying computer game magazines!

The geographical locations of the Czech Republic and Slovakia and their interactive relations with surrounding countries facilitates the spread of viruses, but the situation is far from critical. Almost all organizations (government offices, large banks, and important companies) have worked out their anti-virus policies and use an anti-virus program. The great interest in this issue is reflected in the fact that there are also hundreds of participants at regular anti-virus conferences (in one case, I read, over 600!).

The use of the Internet has increased rapidly during the last two years. The biggest danger comes not from VX web pages, but from the use of electronic mail with attached files. Many Czech and Slovak companies are still not aware of the risks involved in the use of email and so there have been cases where 200 computers belonging to the same organization were infected by CAP in one afternoon. It shows that the scanning of electronic mail is becoming more and more important. The virus problem here is such that there are three anti-virus products for a combined population of about fifteen million – two Czech, *AVAST!* (my product) and *Grisoft's AVG*, and the Slovakian *NOD-iCE* from *ESET*.

The Future

It is always very difficult to predict the future with confidence. However, increasing use of the Internet and further development of operating systems and applications (especially Microsoft's) will definitely influence the virus situation. Local events will probably contribute to it as well, especially as nobody knows what the local virus authors (especially Slovak) will bring out next. Of course, there will be many random factors too. Nevertheless, I believe that anti-virus companies will face up to new viruses, other dangerous programs and threats with the same success in the future as they have done in the past.

COMPARATIVE REVIEW

Scanning on NT

The last time we ran an *NT* comparative review was in September 1997, where we predicted the wider deployment of *NT* as a desktop operating system, rather than as a server platform (see *VB*, September 1997, p.10). It appears we were right, and this current comparative concentrates again on *NT* workstation. Nineteen products were submitted for review, and, as expected, an on-access scanning option is fast becoming standard. Several companies which had not included an on-access scanner with the product submitted for this test claim that the option is scheduled for addition in the next release.

Testing, testing

All tests were run from the Administrator usercode on a standalone *Windows NT 4.0* workstation with Service Pack 3 installed. Boot sector detection tests were run simultaneously with the file-scanning tests, but on another machine, to save time. Sector-level image backups were used to restore the workstation between tests.

The usual *Virus Bulletin* test-sets – In the Wild File and Boot, Macro, Polymorphic and Standard – were used in this review. The ItW sets were updated to the December 1997 WildList, which was the current listing at product submission date (5 January). The standard Clean test-set was used for on-access overhead and on-demand scanning time tests. Generally, default settings were used throughout with the exception that on-access components, where available, were disabled during all on-demand tests. In most cases log files were checked in order to collate detection results. With some scanners it was necessary to use the 'delete infected files' option or to 'quarantine' files.

As in most real-world operation, the scanners faced a large number of uninfected programs in the main speed tests. Here the scanner in question is the foreground application, with *NT's* scheduling set to 'Maximum boost for the foreground application', and no other programs running. This procedure also acts as the false positive test, in which no viruses should be reported.

The complete detection results are reported in the main tables. The results reported in the product summaries are only the on-demand ones, plus the on-access result for the combined In the Wild test-sets.

Alwil AVAST32 v7.70.12 5 Jan 1998

ItW Overall	99.2%	Macro	100.0%
ItW Overall (o/a)	n/a	Polymorphic	95.4%
ItW Boot	100.0%	Standard	100.0%

AVAST32 started out with perfect detection of the ItW Boot set on-demand. The Standard and Macro sets were also perfectly detected, a slight improvement in the macros over the last *NT* comparative. This places *Alwil* with only four other products which scored over 99% In the Wild Overall in this comparative. A good improvement was seen against the Polymorphic test-set.

Although *Alwil* provides an on-access scanner, we could not test its detection rate. This is because, apart from its boot virus detection, it only intercepts attempts to execute potentially infected objects and our testing facility is set up to run tests where the whole system needs rebuilding between each sample to ensure an accurate test.

This was by far the slowest of the scanners tested, six times slower than its nearest competitor, and fifty times more sedentary than its speediest competitor. *Alwil* has opted to give *AVAST32* a very low thread priority, to the extent that a full scan should be almost invisible in terms of overhead on other applications. The clean scan did show up a pair of false positives however, so perhaps this area will be the next to see some very fine tuning.

Cheyenne Inoculan v4.04 15 Jan 1998

ItW Overall	98.8%	Macro	93.1%
ItW Overall (o/a)	93.8%	Polymorphic	90.9%
ItW Boot	98.9%	Standard	99.6%

The on-demand boot test slipped up on the Hare.7610 sample, and caused non-fatal errors on the thirteen samples with less than standard disk formats caused by the virus' meddlings. This slight deviation from perfection was a common thread running through *Inoculan*, and there is a tiny slip from the In the Wild scores of the last outing.

There were improvements – healthy against the Polymorphic test-set and slight in the other on-demand tests. Presentation is of course a strong point, and it must be admitted that there were many features in the package which a workstation-only review cannot address. The missing of small numbers of samples across the board points to a weakness in identities rather than overall mechanics, which is all the more perplexing since this was the most recently built product of all those tested.

Despite a slight difficulty in logging it, on-access scanning was fully supported, and produced similar results to those of the on-demand option. One remarkable feature is that the Polymorphic set was slightly better detected on-access than on-demand. File, Macro and Standard tests dropped two samples fewer than their on-demand counterparts, a creditable result indeed. Scanning speed was at the slower end of the pack, and a brace of false alarms were reported.

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil AVAST32	89	100.0%	629	98.8%	99.2%	744	100.0%	12998	95.4%	887	100.0%
Cheyenne Inoculan	88	98.9%	643	98.8%	98.8%	691	93.1%	12699	90.9%	883	99.6%
Command F-PROT Pro	89	100.0%	621	98.2%	98.8%	744	100.0%	7066	47.6%	887	100.0%
Cybec VET	76	85.4%	651	100.0%	94.9%	744	100.0%	13500	100.0%	887	100.0%
Dr Solomon's AVTK	89	100.0%	651	100.0%	100.0%	744.00	100.0%	13500	100.0%	887	100.0%
EliaShim ViruSafe	86	96.6%	649	99.9%	98.7%	733	98.5%	12823	93.5%	878	99.4%
GeCAD RAV	77	86.5%	507	80.9%	82.8%	485	64.3%	13494	98.1%	821	92.6%
Grisoft AVG	68	76.4%	514	81.9%	80.0%	663	88.3%	11026	81.6%	629	78.6%
H+BEDV AntiVir/NT	87	97.8%	586	92.3%	94.2%	723	96.4%	11455	83.1%	849	96.5%
IBM AntiVirus	87	97.8%	647	99.4%	98.8%	744	100.0%	13000	96.3%	887	100.0%
Intel LANDesk Virus Protect	79	88.8%	623	97.9%	94.7%	744	100.0%	12825	92.5%	861	97.8%
iRiS AntiVirus	88	98.9%	643	98.8%	98.8%	690	93.0%	12699	90.9%	883	99.6%
KAMI AVP	76	85.4%	651	100.0%	94.9%	744	100.0%	13499	99.1%	887	100.0%
McAfee VirusScan	1	1.1%	651	100.0%	65.8%	744	100.0%	13441	98.7%	870	98.9%
Norman ThunderByte	89	100.0%	644	99.8%	99.8%	741	99.6%	13496	98.1%	878	99.2%
Norman Virus Control	89	100.0%	633	99.4%	99.6%	740	99.5%	1296	94.2%	881	99.7%
Sophos SWEEP	89	100.0%	647	99.4%	99.6%	744	100.0%	13495	99.0%	885	99.7%
Symantec Norton AntiVirus	89	100.0%	611	97.0%	98.1%	735	98.5%	11501	84.3%	872	99.1%
Trend Micro PC-cillin NT	84	94.4%	625	98.1%	96.8%	744	100.0%	12883	93.8%	861	97.8%

This leaves the boots, where *Cheyenne's* product was confused by uncommon disk formats, but managed to produce an error for both format and virus, which is to its credit. Consistency between on-demand and on-access detection was maintained since other than these only Hare.7610 was missed. *Inoculan* falls in that middle ground where improvements and declines are as noticeable as they are important.

Command F-PROT Professional v3.01/2.27a

ItW Overall	98.8%	Macro	100.0%
ItW Overall (o/a)	64.2%	Polymorphic	47.6%
ItW Boot	100.0%	Standard	100.0%

F-PROT's speed is among that of the top few and it makes no spurious detections; hardly conversation pieces. Close to the coveted perfect ItW Overall score, missing a handful of file viruses knocked *F-PROT* back to mid-field. The great bane of its detection prowess is, however, the polymorphics. This situation is getting worse monthly, moreover, and the suspicion must be that the imminent v3.0 engine is being developed at the expense of maintaining the older of the species. Standard, Macro and Boot samples, all perfectly detected, back up this theory, requiring not so much an advanced emulator as good scan strings usable by the older *F-PROT*. The odd formats caused no problems in the boot virus tests, though Paula_Boot did throw up an 'unable to read' error on top of a virus alert.

Affairs are not so promising on-access, where boot sector scanning was ignored completely. Polymorphic detection is again a trifle over the on-demand rate with similar comments applying as were warranted by *Inoculan*. Other detection rates dropped due to the need for speed rather than massive detection efficiency. A product which shows its age, and will hopefully have a worthy successor.

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil AVAST32	80	89.9%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Cheyenne Inoculan	75	84.3%	643	98.8%	93.8%	690	93.0%	12750	91.2%	883	99.6%
Command F-PROT Pro	0	0.0%	621	98.2%	64.2%	733	98.5%	7082	47.7%	798	92.6%
Cybec VET	79	88.8%	622	98.4%	95.1%	744	100.0%	12998	95.4%	867	97.9%
Dr Solomon's AVTK	89	100.0%	651	100.0%	100.0%	744	100.0%	13500	100.0%	887	100.0%
EliaShim ViruSafe	0	0.0%	649	99.9%	65.3%	731	98.2%	13163	95.4%	878	99.4%
IBM AntiVirus	87	97.8%	647	99.4%	98.8%	744	100.0%	13000	96.3%	887	100.0%
Intel LANDesk Virus Protect	69	77.5%	623	97.9%	90.9%	744	100.0%	12824	92.5%	861	97.8%
McAfee VirusScan	88	98.9%	530	82.9%	88.4%	688	91.7%	6385	44.7%	767	88.6%
Norman Virus Control	n/a	n/a	424	67.6%	n/a	717	96.6%	7997	44.4%	632	69.1%
Sophos SWEEP	89	100.0%	647	99.4%	99.6%	744	100.0%	13495	99.0%	885	99.7%
Symantec Norton AntiVirus	70	78.7%	611	97.0%	90.7%	743	99.5%	11499	84.3%	841	97.2%
Trend Micro PC-cillin NT	n/a	n/a	625	98.1%	n/a	744	100.0%	12883	93.8%	861	97.8%

Cybec VET v9.61

ItW Overall	94.9%	Macro	100.0%
ItW Overall (o/a)	95.1%	Polymorphic	100.0%
ItW Boot	85.4%	Standard	100.0%

The product for the people to whom velocity is almost everything, *VET* churned through the 500 MB of the Clean test-set in a mere 102 seconds, yet still showed an impressive on-demand detection rate. The detections against the In the Wild File, Standard, Polymorphic and Macro test-sets all gained the much sought-after full marks, so far so good.

Those who crave speed so much may, of course, have no desire for lowly 3.5-inch disks, which is where *VET* failed to deliver. *VET* detected all boot sectors it saw on what it considered valid disks, but failed to recognize thirteen of the samples as actually being on any sort of valid diskette, and unworthy of its attentions as a result. These are real viruses which can infect on boot-up, despite the inability of the operating system to access data stored upon the diskettes involved. This problem has been addressed before in *VB* reviews, and here prevents the attainment of a VB100% award by *Cybec*.

Curiouser and curiouser, *VET* is clearly able to scan these types of boot sector, as the on-access scanner failed to spot a completely different selection of undesirables. There was a slight slippage seen in all other categories except the Macro test-set, where full detection was achieved. This turns out to be the most common area where full scores are possible, a reassuring thought in corporate settings where macro viruses are more commonly encountered than other types. Reassuring for *Cybec* is the fact that, theoretically, their product *can* detect all viruses in *VB's* test-sets, but *VetNT* needs some reworking to do so.

Dr Solomon's AVTK v7.79 1 Dec 1997

ItW Overall	100.0%	Macro	100.0%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	100.0%

Virus Bulletin's considered opinion was that the *NT* comparative would produce fewer VB 100% awards than the recent DOS equivalent. The full extent of this prediction is more significant than expected. All this is of course verbiage, for *Dr Solomon's AntiVirus Toolkit* detected everything in every set and did so both on-demand and on-access. It is the only product to receive a VB 100% award in this review.

With a speed that lies in the firmly efficient range rather than fast or slow, there is of course room for improvement if such has to be found, and a product is never really perfect until the last virus is written. Enough philosophy, roll on the next product.

EliaShim ViruSafe v2.5

ItW Overall	98.7%	Macro	98.5%
ItW Overall (o/a)	65.3%	Polymorphic	93.5%
ItW Boot	96.6%	Standard	99.4%

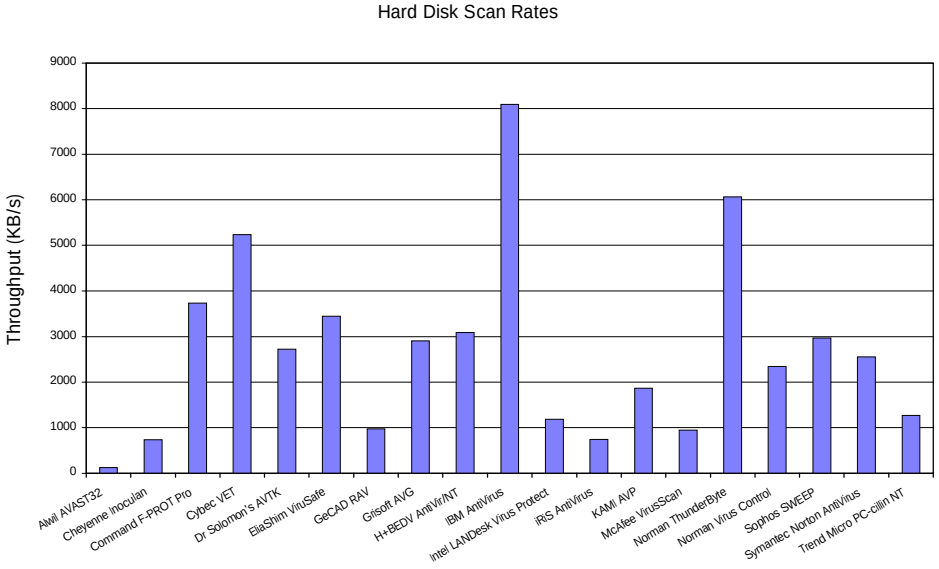
Tantalizingly close to omniscience in the on-demand tests, on the whole *ViruSafe* is the sixth consecutive product whose performance would have been seen to be remarkable two years ago. With the increasingly high expectations of the anti-virus market, and the efficiency of the engines used to meet these expectations, *EliaShim's* program is in the upper echelons, with a good few close competitors.

The detection rate has increased from its last outing, into the high nineties in all fields, and just a slight improvement will produce a few fully-detected test-sets. Boot sector detection, for example, was thrown by three variants of Hare which should be expected and detected in the future. With such jostling for the top spot, any faults are of vital importance, and *ViruSafe* falls down on false alarms. Similar to its DOS scanning, the scanner threw up twenty five cases where Cruncher-4000 was detected *in absentia*. Despite this being done in a respectable time, it is still a considerable flaw.

EliaShim is the third of this month's products to be more effective against the polymorphics when using on-access scanning. In contrast, on-access scanning does not apply to boot sectors, and changes to other categories are in the expected range of small drops in detection.

GeCAD RAV v5.20

ItW Overall	82.8%	Macro	64.3%
ItW Overall (o/a)	n/a	Polymorphic	98.1%
ItW Boot	86.5%	Standard	92.6%



GeCAD's RAV is relatively new to *VB* tests, and this is its *NT* comparative debut. It is the first, alphabetically, of six products not to include an on-access scanner. Despite its Romanian provenance, the program suffered no problems in translation, but several in implementation.

The detection rates were not high, with the exception of the Polymorphic set. 98.1% detection here places it an impressive fourth amongst some lofty company. Speed is a little on the sluggish side, and 33 false alarms are far too many.

All this accepted, the real problems came in the boot sector test, where buffering problems proved a nightmare. Each diskette was only detected as being virus-ridden once, and then not again until a different virus had been tested. Worse still, if for example, a Stoned variant was tested, it caused other successive, but different, Stoned variants to be ignored until a different family had been interpolated into the series. Somewhat disturbingly, the error message 'there is something missing please verify a:' appeared consistently during testing, and detection seemed to fail when the program was present as a tray icon. Problems there are, but promise too, and it must be remembered that some of todays high fliers made less than stunning debuts.

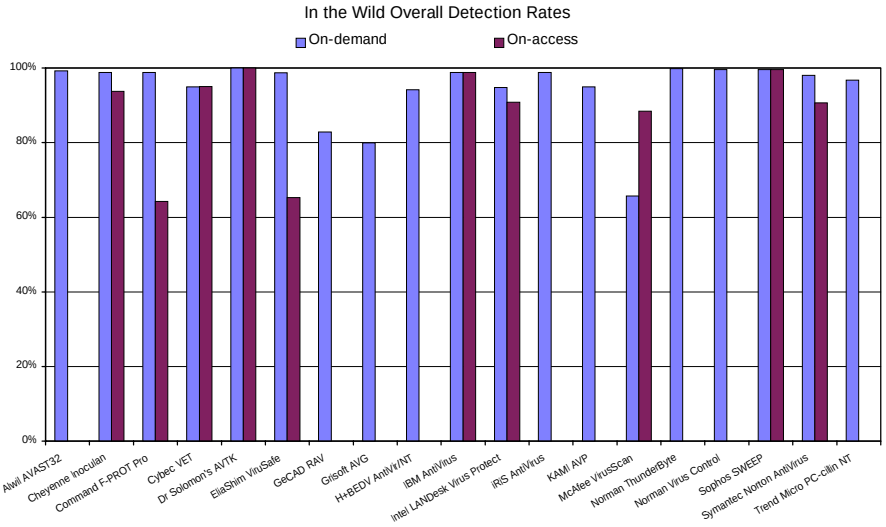
Grisoft AVG v5.0 (Build 1207)

ItW Overall	80.0%	Macro	88.3%
ItW Overall (o/a)	n/a	Polymorphic	81.6%
ItW Boot	76.4%	Standard	78.6%

Another Eastern European product relatively new to *VB* tests, *AVG* claims resident-protection for its product, which is designed to serve both *Windows 95* and *NT* equally. Some platforms are more equal than others however, and the resident-protection is in the form of a VxD – which of course does not work under *NT*. On a happier note, *AVG* saw no aberrations in the Clean test-set, which it ran through in an entirely respectable 185 seconds.

Detection rates were very similar to those seen in the DOS comparative review in the February issue, with the In the Wild Boot test-set being the particular sticking point once more. *AVG* failed to read any of those disks with less than absolutely standard formats, and thus dropped down by the unlucky thirteen into the realms of poor performance.

The detection rates in the comparative give an overview, but the standalone review on p.18 of this issue supplies a much fuller description of the nuts and bolts of the program. *AVG's* user interface is consistent across the two platforms.



not spectacular, with the expected lack of false positives. The mandatory checksumming technique meant the first run through the Clean set took 240 seconds (2225.5 KB/s).

IBMAV's on-access scanner claimed to detect viruses only in boot sectors, in memory or upon execution. This is presumably a simplification, since the on-access scanner picked up exactly the same specimens that its on-demand counterpart found. The on-access scanner does not name infections, suggesting you run the on-demand scanner instead. During testing, there was a perverse hope that the on-access scanner would detect some of the on-demand missed samples just to see the resulting confusion. Another product for whom the full set was close but not quite there.

H+BEDV AntiVirNT v5.10.01 10 Jan 1998

ItW Overall	94.2%	Macro	96.4%
ItW Overall (o/a)	n/a	Polymorphic	83.1%
ItW Boot	97.8%	Standard	96.5%

With a longer-established product than the previous pair, *H+BEDV* have yet to translate their help files into English, though menus, general instructions and icons are available in either German or English. *AntiVirNT* has no on-access scanning function. Speed-wise it kept with the pack, though five suspected viruses in the Clean set was a little disappointing. This product certainly won the 'added messages available in the clean scan' award, producing warnings of damaged files, and an over-large COM file in addition to the viruses supposedly spotted.

The CRC function in the program was not tested, leaving the usual collection of on-demand tests to contend with. The boot sector tests missed the perennial favourites of Moloch and Hare.7750, but found no trouble at all in spotting the hidden evils on the disks having possibly tricky formats. This gave a much improved set of detection figures over the September *NT* comparative, which was to a lesser extent carried over to the other test-sets. It is to be hoped that such improvement can be maintained.

IBM AntiVirus v3.02w

ItW Overall	98.8%	Macro	100.0%
ItW Overall (o/a)	98.8%	Polymorphic	96.3%
ItW Boot	97.8%	Standard	100.0%

Another big company, faring as befits its size. Against the In the Wild File set only Win95.Anxiety evaded *IBMAV*, but with two samples of Hare in the boot test this was enough to dash any hopes of 100% In the Wild detection. Polymorphics saw Cryptor.2582 the only failure, though a full set of failures admittedly, but besides these *IBMAV* detected all samples in the non-ItW test-sets. Speed was fine, though

Intel LANDesk Virus Protect v5.01 16 Dec 1997

ItW Overall	94.7%	Macro	100.0%
ItW Overall (o/a)	90.9%	Polymorphic	92.5%
ItW Boot	88.8%	Standard	97.8%

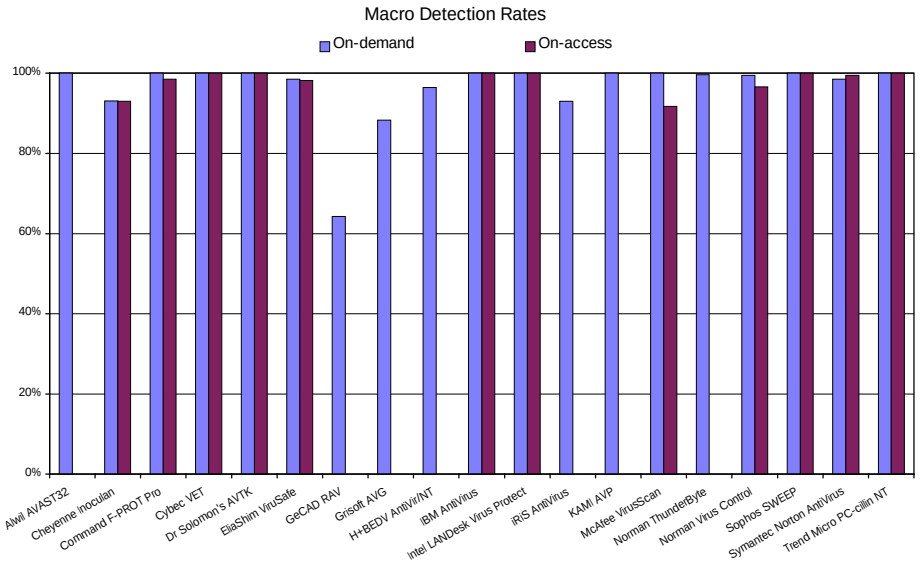
Intel suffered once more at the hands of the boot sector test. Thankfully this was simpler to discover than in some programs, multiple disk scanning being a feature more common in DOS products but supported well here. Unfortunately, *LANDesk Virus Protect* was unable to detect a selection of rather aged viruses still in the wild, again including the venerable Stoned-standard which caught it out in the previous *NT* comparative. A perfect score on the Macro test-set is encouraging, and on-demand scores against the other three test-sets were respectable but hardly earth-shattering in their magnitude.

On-access results were pretty much the same as the on-demand ones in the Macro, Polymorphic and Standard sets. In the Wild File was a little worse for on-access detection than on-demand. Similarly, the added problems with boot sectors came as no shock. Once more the errors thrown up by strange formats prevented detection of any viruses on a fair number of the samples. This took *LANDesk* to the bottom of the stack for programs with operating on-access boot scanners. As for speed, *LANDesk* is one of the more ponderous of the products, and it still manages to discover four viruses in places where they do not exist.

iRiS AntiVirus v22.03 16 Dec 1997

ItW Overall	98.8%	Macro	93.0%
ItW Overall (o/a)	n/a	Polymorphic	90.9%
ItW Boot	98.9%	Standard	99.6%

No on-access scanner here, and a display of on-demand scanning which would impress but for the better scores common in this review. At 720 seconds, *iRiS AntiVirus* required longer than average to scan the Clean test-set. Somewhat bizarrely, the program claimed that it had been altered when run, though we did not count this as a false positive to add to the two generated against the Clean set. Remembering that in the past *iRiS AntiVirus* has produced up to 139 false positives this shows a massive improvement somewhere in the code. This apart, the program operated as expected, and missed only the Hare.7610 on the boot test.



Detection rates were somewhat down from previous *Windows NT* incarnations of *iRiS AntiVirus*, though this can with hope be ascribed to the rather old scan string files submitted for testing. On a more positive note, polymorphic detection was up significantly, an area of noted weakness last September.

KAMI AVP v3.0 (Build 117) 5 Jan 1998

In the Wild Overall	94.9%	Macro	100.0%
In the Wild Overall (o/a)	n/a	Polymorphic	99.1%
In the Wild Boot	85.4%	Standard	100.0%

Rumours of great changes afoot at *KAMI* are clearly not based upon any great problems with the product as can be seen by these results. *AVP* fell well within the commonest range of speeds at 286 seconds, and threw up no false alarms, an improvement upon the previous *NT* comparative. This improvement was apparent in all facets of the detection ability of the program, which missed just one sample of DSCE.Demo in the Polymorphic test-set. The boot sector problems, on the other hand, remained much the same as before. Failure to read the thirteen confusing disks without producing errors prevented *AVP* from displaying its full ability to detect In the Wild Boot samples.

A slightly confusing artifact could also be generated if infected disks were interrupted in scanning after they had been declared infected on screen. Under these circumstances a clean disc inserted and scanned would produce a large red infected notice. With these results such niggles are not, however, a major issue.

McAfee VirusScan v3.1.4 11 Dec 1997

In the Wild Overall	65.8%	Macro	100.0%
In the Wild Overall (o/a)	88.4%	Polymorphic	98.7%
In the Wild Boot	1.1%	Standard	98.9%

McAfee VirusScan proved one of the more interesting products to test. The on-demand scanner was effective at spotting all In the Wild Files and macro viruses in the test-sets used, and put in a creditable 98.7% score in the Polymorphic set. Speed of scanning is at a rather plodding rate, but nothing was detected that should not have been. On-access the polymorphics proved rather too elusive to *VirusScan*, though detection of other file infectors was fair. This leaves the boot sector viruses. Of the 89 boot sector viruses provided, *VirusScan* detected just one on-demand. Yes, one! We were surprised too.

VB has no great wish to be sued, and so we checked this, and came to the following conclusion. ABCD, the boot virus that was detected, is on the only diskette that contains a file (a relic of an atypical replication procedure). Sure enough, if a file is placed on other boot virus test diskettes, *VirusScan* inspects the diskette properly. With no files present it returns the error 'Path A:\ does not exist' and fails to look at the boot sector.

Consider the misinformed but ubiquitous Joe Bloggs, who 'knows' that deleting all files on a disk will destroy viruses on it – if he performs this task *VirusScan* could incorrectly agree that he has been successful. This bug will also see *VirusScan* fail to detect boot infections on new, pre-formatted but infected diskettes.

At this point optimists are allowed to mention the detection rates on-access. These are a bit better, though suffering like *RAV* from a buffering problem which makes detection possible, if somewhat hit and miss. The on-access scanner is on by default, so a user would have to turn it off deliberately. In a compounding sin, however, the resident program makes scanning boot sectors an unstable affair at best. The scanner crashed *NT* to a featureless desktop no fewer than seven times in the boot sector testing process, and not on any particular subset of disks. Joe Bloggs might take this as a fair enough reason to turn off the on-access scanner – you can imagine the rest.

Norman ThunderByte v8.04 29 Dec 1997

ItW Overall	99.8%	Macro	99.6%
ItW Overall (o/a)	n/a	Polymorphic	98.1%
ItW Boot	100.0%	Standard	99.2%

After such a set of comments it takes something special to be noticed. *NTVC* can thankfully provide this however, in the amazing speed at which it scanned the Clean set. Eighty-eight seconds represents over 6 MB/s and with no false positives and without the assistance of checksumming, as used by the only faster product, is a very creditable result. In all test-sets, *NTVC* missed a smattering of samples – at the risk of being repetitive, close but no cigar.

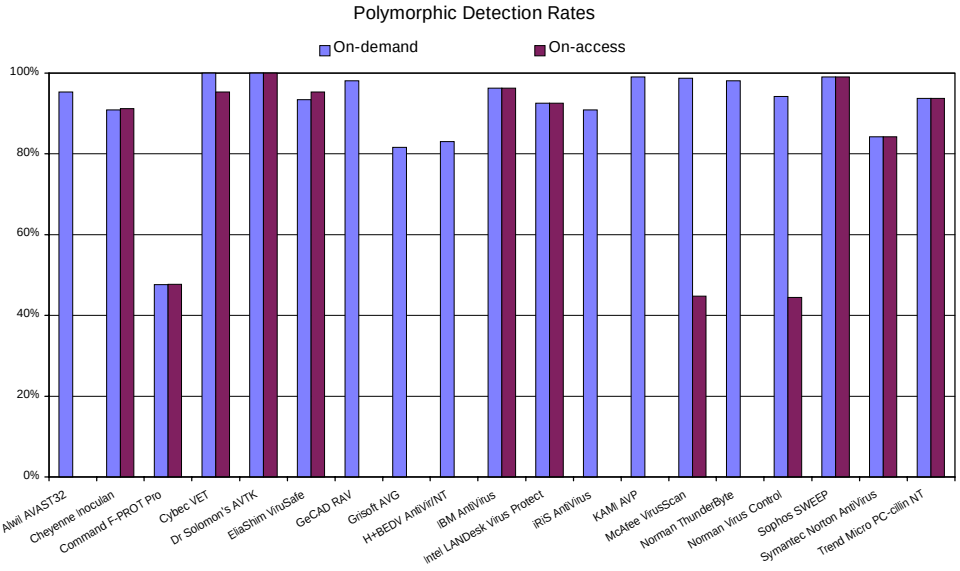
NTVC provides no on-access scanner, but instead supplies an installation checksum routine and scheduled background scanning. Neither were tested in this review.

Norman Virus Control v4.30a 5 Jan 1998

ItW Overall	99.6%	Macro	99.5%
ItW Overall (o/a)	n/a	Polymorphic	94.2%
ItW Boot	100.0%	Standard	99.7%

The last false alarm reared its head in a middle-ranking speed test from *NVC*. On-demand, *NVC* is efficient but failed to deliver the raft of 100% results we have seen from its brethren in recent comparatives. Responsibility for this is entirely attributable to its failure to detect all eighteen samples of Morphine.3500. Polymorphics were also less comprehensively detected than is ideal, despite improving considerably over the last three months.

Testing *NVC's* interesting approach to on-access virus protection, involving behaviour blockers and other mechanisms, is beyond the scope of this review. The only 'traditional' on-access scanner is the macro detector, Cat's Claw.



This component did not quite detect as many macro viruses as the on-demand scanner. Logging of on-access scanning was less controllable than suggested. This proved a common flaw in the tested programs, too many of which, on-access, relied upon binary log files, or provided no log file.

Sophos SWEEP v3.05 5 Jan 1998

ItW Overall	99.6%	Macro	100.0%
ItW Overall (o/a)	99.6%	Polymorphic	99.0%
ItW Boot	100.0%	Standard	99.7%

A good result for *Sophos*, but a definite downturn from past near-perfect detection. *SWEEP* missed the new ItW File virus Win95.Anxiety and, mysteriously, five samples of Neuroquila.A from the Polymorphic test-set. The latter is surprising given that *SWEEP* has consistently detected all samples in this test-set for many reviews. In the Standard set Positron was undetected, which is almost certainly by design as it has been the lone, missed sample from the Standard test-set for several consecutive comparatives.

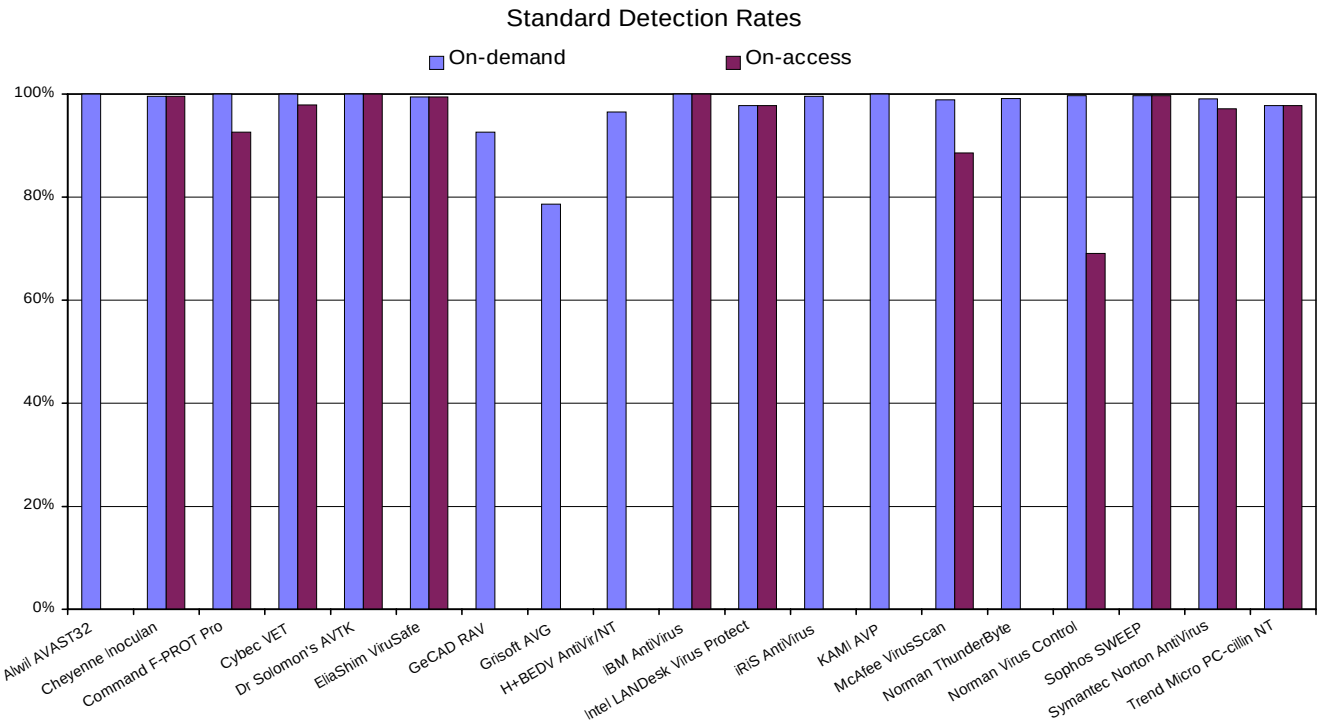
SWEEP's on-access component proved the only equal to *Dr Solomon's* in detecting all boot sector viruses, and like *AVTK* and *IBM AntiVirus* the results obtained by on-access and on-demand scanning were exactly comparable. Speed on-demand was neither good nor bad, and the clean files were all correctly reported as uninfected.

Symantec Norton AntiVirus v4.0

ItW Overall	98.1%	Macro	98.5%
ItW Overall (o/a)	90.7%	Polymorphic	84.3%
ItW Boot	100.0%	Standard	99.1%

NAV's discovery of all samples in the on-demand boot test continues its good, recent record there. Detection of Standard test-set viruses has improved, yet in other on-demand areas the new specimens proved problematic for *NAV*. No false positives were produced on the other hand. Scanning speed was decidedly average.

Worse news was in evidence with the on-access boot tests, where a combination of simple misses and inability to access diskettes gave rise to nineteen misses. As an addition to these imperfections, the buffering syndrome similar to that seen with *GeCAD RAV* and *McAfee VirusScan* was again apparent. Results other than these were comparable to those of the on-demand tests.



Trend Micro PC-cillin NT v1.0 VPN 347

ItW Overall	96.8%	Macro	100.0%
ItW Overall (o/a)	n/a	Polymorphic	93.8%
ItW Boot	94.4%	Standard	97.8%

Trend's PC-cillin NT suffers a little by being at the end of the alphabetical trail, where it nevertheless manages to raise some points not yet addressed. On-demand Macro detection was a perfect 100%. The three Hare variants, Moloch and Neuroquila.A were the only misses in the on-demand Boot sector test. Though the scan speed is slower than average, it was by no means frustratingly so, and threw up no false positives. *PC-cillin's* other on-demand results were unexceptional by dint of resembling those of other products.

The on-access scanner does not test for boot viruses, but all other test-sets were detected equally well on-access and on-demand. Given how few products detected (and missed) the same viruses in on-access as in on-demand modes, this is actually an encouraging result, in terms of what it says about the product's developmental consistency.

Conclusion

A comparison with last month's DOS comparative shows, perhaps not surprisingly, that *NT* products handle macro scanning more effectively than their DOS-based brethren. Unfortunately, it appears that the macro detection gains are the roundabouts to the boot virus swings.

This is our third *Windows NT* comparative and this is the third time we have shown the general inadequacy of certain approaches to dealing with boot sector viruses under this operating system. Although supplanted as commonest by some macro viruses, boot viruses still account for a significant slice of infections reported in our monthly Prevalence Tables. Moreover, we still receive many panicked reports of infected systems – clearly many users are still not using the common, BIOS-based against protections. Thus, reliable detection of these viruses is still important. We hope to not have to repeat this complaint in the next *NT* comparative.

An interesting feature of the current results is how the recent appearance of Win95.Anxiety and its relatively rapid appearrance in the WildList had such a major influence on the ItW File detection results. Although not necessarily the sole malefactor, it was missed by ten of the products tested, and was the single detractor from a perfect ItW File score for two products, denying one of them a VB 100% award. Another new entrant to the ItW File set, which also acted as a spoiler for many, was Morphine.3500, again contributing to the collapse of ten products' VB 100% hopes.

Congratulations to the *Dr Solomon's* team for their second consecutive perfect score across the board.

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 NT v4.0 (SP3)*. The workstations could be rebuilt from disk images and the test-sets were held in a read-only directory on the server. All timed tests were run on one workstation.

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

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NT/199803/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

PRODUCT REVIEW 1

AVG v5.0 for Windows 95

Dr Keith Jackson

Czech developers *Grisoft* claim that *AVG* is 'a sophisticated antivirus system for detecting and removing viruses'. The product can operate under DOS, *Windows 3.1*, *Windows 95* and *NT*, or across a network. However, this review only covers the standalone *Windows 95* version.

Installation

AVG was provided for review on three 3.5-inch, 1.44 MB floppy disks. In fact, two identical sets of disks were provided – I know not why.

Installation was initiated by executing SETUP.EXE. After reading warnings about the licensing conditions, I had to enter my name, a company name, and the program serial number before installation could proceed. The name of the subdirectory where *AVG's* files were to be stored could be altered if required, and an option was provided to install *AVG's* memory-resident component. The usual bargraphs whirred, the other floppy disks were requested, and a reboot was performed. All in all a painless program installation, much as we have come to expect.

Documentation

AVG arrived with three small A5 books entitled 'Installation and First Steps', 'User Manual', and 'Computer Viruses and You'. The titles are fairly self-explanatory. The 'Installation' booklet is very short and to the point. It contains just over eight pages, nearly half of which are taken up with the licence conditions and details of the warranty. This manual can be succinctly summarized thus: use the floppy disks, follow the instructions to install the *AVG* software, and do not forget to read the licence conditions (or else…).

Speaking of the *AVG* licence, it contains some very odd clauses; for instance, the product is not sold, it is licensed for a period of time, which is fairly standard. However, all parts of the packaging must be kept for when the licence expires, which is presumably when you no longer require the product and stop paying for upgrades. The licence explicitly includes 'the wrapping of the distribution package' in the list of things that must be retained for subsequent return to the vendors.

Lawyers are wonderful – just when you thought that they might inhabit the real world after all, they come up with nonsense like that and shatter the illusion. Hands up all those users who not only keep the box in which a software product is packed, but also keep the wrapping paper. Nobody? I thought so.

The licence also includes a wonderful cop-out which states that (and I quote) 'The manufacturer does not guarantee the perfect operation of the system if the system is used on equipment not 100% compatible with a standard IBM PC'. Note that no attempt is made to define a 'standard IBM PC'. Nor could it be, such a beast no longer exists – if it ever did. When things get rough any half-decent lawyer has enough in that one phrase to defend the developers of *AVG* against anything. Absolutely anything.

The User Manual is well written, but suffers somewhat because it applies to several versions of *AVG*, running under various operating systems. This inevitably makes it vague on detail. Still, given that many (most?) anti-virus vendors seem to have given up on manuals completely, at least *AVG* provides something in printed form.

'Computer Viruses and You' a slim, A5 volume, contains a good description of computer viruses, how they operate, their history, and the parts of the PC that they attack. It would be especially easy for a first-time user to follow the explanations provided.

Interface

In last month's review I complained that all *Windows 95* anti-virus software looked the same. No sooner had the words tripped off my keyboard and into print, than something comes along that looks completely different.

Down the left hand side of *AVG's* main window a list of section headings is provided ('Tests', 'Utilities', 'Help' etc). Each of these headings can be expanded (by double clicking on it) to reveal the options available within that section. Once an action has been selected, activity takes place in the main part of the window, while there are

AVG's user interface breaks the mould somewhat, but is an eminently usable design.

several large buttons across the bottom edge. It is refreshingly different from the usual drop-down *Windows* menus, and it works rather well.

Heuristics

A short excursion into *AVG's* heuristic capability is called for at this point. One of the main components in *AVG's* armoury is its 'Complete Test'. This option scans everything, using both an ordinary scanner and a heuristic scanner. If *AVG* is sure that a particular file is 'clean', it adds it to the 'validation database'. Future 'Complete Test' activations need only scan files whose checksums have changed since the database entry was created, with a consequent reduction in scan time. *IBM's* scanner uses the same tactic.

So far, so good. However, the *AVG* documentation warns that the heuristic scanner can produce false alarms, and sure enough it does. Before installing *AVG*, I re-installed *Windows 95* on my test PC. Therefore, the only files on the C drive were either from *Windows 95*, or they were installed by *AVG*. The first time I requested a 'Complete Test', *AVG* found that three of the *Windows 95* files were infected, two by an unknown virus. More worryingly, one file was thought to be infected by the 'LSD' virus.

The first 'Complete Test' execution took 1 minute and 2 seconds to execute, having tested 800 'objects' (their word). The second and subsequent executions took just 22 seconds to complete, with the same three COM files found to be infected.

Scanning

I tested *AVG's* detection capabilities against the *VB* test-sets (see the 'Technical Details' section below) which are stored on CD-ROM. The *AVG* scanner stated that it detected 514 of the 549 samples contained in the In the Wild test-set (93.6%). Frankly, this figure is disappointing; it should be closer to 100%. When the heuristic scanner was used, the detection rate increased to 95.6%, or 525 of the ItW test files. This was better, but still nowhere near 100%, which belied many of the claims made for the efficacy of the heuristic scanner. Heuristic detection still had one trick up its sleeve – a 'sensitive' mode of operation, but this did not increase the number of viruses detected.

However, the above result was better than the 536 out of a possible 774 viruses (69.2%) that the *AVG* scanner detected against the Standard test-set. Once again the heuristic scanner improved things somewhat, but it only raised the number to 713 (92.1%) when the 'default' heuristic was used ('sensitive' heuristic detection obtained exactly the same result).

When the 716 files of the Macro test-set were scanned, no matter which method of scanning or what type of heuristic scanning was used, the result was always the same – 650 were detected as being infected (90.7%), i.e. heuristic detection does not increase the chance of detecting a macro virus. This is perhaps unsurprising, and many products exhibit exactly the same property.

The Polymorphic test-set contains 13,000 viruses (500 samples of 26 viruses), and the *AVG* standalone scanner detected 10,526 (80.9%). Heuristic detection fared better, raising the detection rate to 11,996 (92.2%). This result remained the same no matter whether 'default', or 'sensitive' heuristic detection was used.

In the Wild Boot sector virus detection was a little better at 94.5% (86 from 91), but this is a test where you should expect 100% detection.

False Alarms

When I tested *AVG* 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 infected with a virus), it did not find any virus infections. Given that *AVG* had informed me that three *Windows 95* files were infected (see above), this result seemed rather curious.

Speed

Using its default settings, *AVG* scanned the C: drive of my test PC in 20.9 seconds. It is interesting, and highly confusing, that this is actually faster than the 22 seconds quoted above for a 'Complete Test' during which only the files that have been altered are actually scanned. What is the point in having the 'Complete Test' inspect its validation database if this process is slower than actually scanning the files? Most odd.

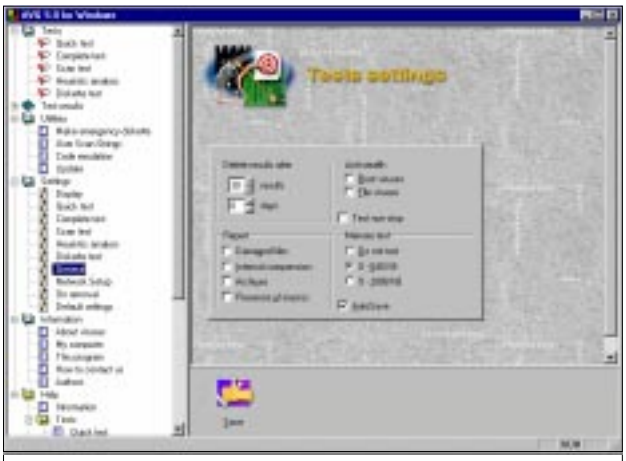
I scanned inside internally compressed files (the scan time went up to 23.6 seconds), and inside archive files (ZIP, ARJ etc.), which further increased it to 28.3 seconds. Finally, I used the heuristic scanner, and this pushed the scan time to 51.1 seconds.

For comparison purposes, the DOS version of *Dr. Solomon's Anti-Virus Toolkit* took 57 seconds, and the DOS version of *SWEEP* from *Sophos* 48 seconds, to perform the same scan. *AVG* is no slowcoach, it whizzes along much faster than competitor products on the market.

Memory-resident Scanning

The memory-resident scanner provided with *AVG* can be set up to check floppy disks or files and to ask the user what to do if an infection is found. Note that I have not mentioned any options that can tailor how this software actually operates – there do not appear to be any.

The control program for the memory-resident software still has a few obvious bugs. Click the 'schedule' tab and the program closes. This is not exactly an endearing habit. Likewise, the boxes that activate scanning of floppy disks and/or files can be activated from almost anywhere along a



The general settings page is one of the many pages of configuration options.

horizontal line stretching out from the box itself, through its title, and on towards the right-hand side of the window. The invoice for my consultancy fee is in the post!

AVG's memory-resident scanner checks for viruses while infected files are being copied from one location to another. It seemed reasonable at detection, although absolute figures are hard to come by as it always interrupted a file copy whenever an infected file was found.

I waded through hundreds of individual keypresses for the ItW test-set, only to find that after 248 viruses had been detected, the screen informing me of a virus detection was replaced by a series of apparently randomly-coloured rectangles. This is called a software bug.

As expected, the memory-resident software was far less efficient at spotting polymorphic test samples. Indeed, it had got about one third of the way through copying the entire 13,000-strong Polymorphic test-set before it detected a single file as being infected.

When I tried to delete files that had been used in this copying test, the memory-resident software indicated files that were in the *Windows* Recycling Bin as infected. This may be thorough, but it is also a thorough nuisance. There should be an option available to disable this action.

The Rest

A 'Quick Test' can be executed which just looks at the disk locations and files that are deemed to be either important, or likely to be infected. This list can be tailored by the user. Using its default settings the 'Quick Test' option checked the C: drive of my test PC in about one second, almost too quick to measure. It really lives up to its name!

A specific menu option is provided to check out floppy disks. I like this idea – many a time I have wrestled with a product's intricate menu system trying to find out how to scan a floppy disk. Having an easy way to kick-start this process is a real boon.

On-line information about viruses, and families of viruses, is provided. What is there is very helpful, easy to understand, and most comprehensive. However, there are about 170 names of individual viruses in the list entitled 'Virus Information'. Some of these contain more than one entry, but even so this does not even begin to compare with the total of well over 10,000 viruses of which many scanners claim knowledge.

Finally, utilities are included to make an emergency diskette, introduce scan strings entered by the user, update the software, and run something called 'Code Emulation'. This last facility allows 'expert' (*Grisoft's* word) users to analyse suspicious programs by stepping through their code with the emulator from the *AVG* heuristic engine – not for the faint-hearted this one.

Conclusion

Face facts – the basic detection rate of *AVG* needs some more work. Competitor products are much better at the core task of detecting viruses. Having said that, the operational aspects of *AVG* are good, it is a delight to use, works very quickly indeed, and provides all the usual features.

The developers of *AVG* are probably perfectly well aware of these conclusions; they must know their current 'hit rate'. It is obvious in their own 'Virus Information' section, which is somewhat short on content. The question is – are they prepared to put in the sheer number of man hours that are required to increase the virus knowledge incorporated into *AVG*? We shall see.

Do not even consider purchasing *AVG* unless the developers agree to remove the 'standard IBM PC' clause from their licence. It is onerous and makes it impossible *ever* to have a legal claim against the developers. Likewise, unless you have a fetish for collecting waste paper, insist that the clause about keeping the product's wrapping paper for ever and a day is removed from the *AVG* licence – it is just daft.

Technical Details

Product: *AVG v5.0 for Windows 95*.

Developer: *Grisoft Software Ltd*., Lidicka 81, 602 00 Brno, Czech Republic, Tel +420 5 4124 3865, fax +420 5 4121 1432, BBS +420 5 4124 3858, email: grisoft@grisoft.anet.cz, WWW http://www.grisoft.com/.

Availability: *AVG* requires at least 5 MB of hard disk space.

Version evaluated: 5.0P, build number 1207, resident VxD driver version 1.7.

Serial number: 50U-1-102955-MVJ.

Price: Licence price for single user $49, with a sliding scale to $30 per licence for 51 to 100 users. Large volume discounts can be negotiated with the vendor.

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 run *Windows 95*, *Windows 3.11*, *Windows 3.1*, or DOS 6.22.

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

PRODUCT REVIEW 2

Command AntiVirus for NetWare v4.0

Martyn Perry

Although *Command AntiVirus* (*CSAV*) draws heavily on its predecessor, changes are being made to differentiate it from *Command F-PROT*. However, in this period of transition, some screens show *CSAV* information while the console commands still refer to *F-PROT*. Similar quirks are also found throughout the documentation.

Presentation and Installation

The software was supplied on four floppy diskettes. You have two installation options. The first is to install directly at the server console, but this does not install the Windows Administration program. The other option is to install from a workstation. I chose the latter, using InstallShield to handle the installation options. The first screen of the workstation installation presents a choice of components: Command AntiVirus Server Files, Command AntiVirus Client Files, AlertTrack Server Files, and AlertTrack Client Files. Initially, just the first two options were chosen.

The default folder for the program files for the workstation is still set to C:\F-PROT. Incidentally, if the installer has not logged in and starts installing software, 'Error -1 cannot create server list' comes up when loading the second disk. After clicking OK, the installation reports 'Set-up complete' at this point. The software is idiot-proof but not quite reviewer proof!

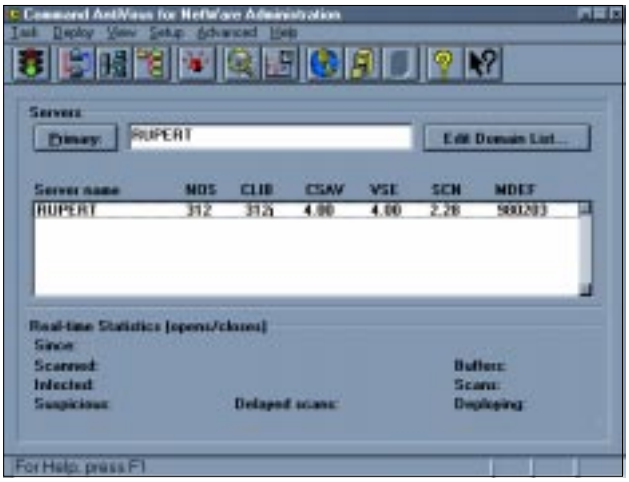
Next, the target server directory for NLM files must be selected (the default is \\SERVER\SYS\SYSTEM\F-PROT). At this stage, there is the option to add a 'LOAD F-PROT' line to the server's AUTOEXEC.NCF file. Having performed the main installation, all that remains is to install any updates to the virus signatures.

Command AntiVirus for NetWare

Loading the NLM without any command line, options, it creates the daily scan options. The load-time option NoDailyScan prevents this from happening. Other load-time options include setting the server utilization level to something other than the default of 40%, changing the maximum number of buffers (default 20), and choosing whether to save infected files.

There are four ways of controlling the server software, the first being to use the console command line. This will display a table of the various options available from the console. Secondly, FPNCON.NLM provides a menu-driven version of the console commands. Thirdly, the F-PROT.INI configuration file can be edited. This can contain settings for Log File, Global Settings, Real-Time scanning, Manual scanning, Scheduled scanning and Reports.

After modifying the F-PROT.INI file, the running NLM must be re-initialized for the changes to take effect. This can be done in three ways, the first being to unload then reload the NLM. The second method is by issuing the console command 'F-PROT REI', and the third, and most convenient method, is to use the Windows Administration program from a workstation. This is also the fourth method of controlling the server software, alluded to above.



The *CSAV* scanner provides the usual three modes of operation – Immediate, Scheduled and On-access (Real-time). In addition, there is a Global option which allows all three modes to be updated with an identical setting without having to visit each one in turn. These override the ready-to-go or hard-coded settings shipped with the product. The former are a set of options pre-defined to handle most of the routine activities required of a scanner.

A number of configuration options are common to all three scan modes and can be defined under Global Defaults. The Include List not only contains the default file extensions but can also contain volumes, directories and specific files. Default file extensions are: COM, DO?, DRV, EXE, FON, OV?, PGM, SYS, XL?. There is a separate Exclude List for volumes, directories and files to be ignored during a scan. Three exclusions are made by default, but not displayed. These are SYS:BACKOUT.TTS, NetWare bindery files, and any quarantine directory you may have configured.

Scanning Options

In the case of Immediate scanning, a specific path can be defined just prior to running the scan. The actions available if a virus is detected are various. Quarantine moves the file to the chosen directory (default QUARANT.INE), Delete

removes the file, and Rename changes the first character in the file extension to 'V', unless it already is 'V', in which case '!' is used instead. Further actions include Disinfect, which attempts to clean up the infection, and Report, which simply adds the information to the log file.

When Quarantine, Delete or Disinfect are selected, a copy of the original file is put in the quarantine directory using a hexadecimal number for identification. This is the default action on virus detection unless the SAVE option is used when the software is first loaded.

You can choose on-access scanning of files when they are opened, closed, or both. To relieve the load on the server, when a file is closed and has been modified, it is put in a queue to be scanned within a five minute window. Should the file be re-opened during this period, it is automatically scanned even if scan on file open is disabled.

Multiple scheduled scans can be set up independently with a description to identify the scan options and the item to scan. Scans can be scheduled by frequency or by period, including Daily, Weekly, Monthly or Quarterly. Alternatively, a delayed scan can be defined with a period of Hours, Days, Weeks or Months.

The duration of scheduled scans can also be configured, and there are three options in case a scan runs past its defined stop time. 'Finish' continues scanning until completed. 'Wait' stops the scan and remembers which files are still to be scanned so the next time that scanning configuration is run it picks up from where it left off. Finally, 'Quit' stops the scan at the appointed time – re-running this scan will cause it to start from the beginning.

Administration

As stated earlier, changes to configurations can be performed from the server console, by editing F-PROT.INI, but more usually from the administration workstation.When the Administration program is first called, it requests the selection of the primary server and whether to display all *CSAV* servers or just the domain controllers. There are also facilities for deploying software upgrades from a master server to other servers.

Reports and Activity Logs

A number of logging options are available. F-PROT.HST keeps a history of files that have been quarantined, deleted or disinfected. These actions are denoted by 0, 1 or 2 respectively in the report along with the hexadecimal name of the file and its original location. This information can be used in conjunction with the hexadecimal value of the file name to identify the original name and location.

F-PROT.LOG contains the results of the scans performed with summaries for manual and scheduled scans. To control the size of this log file, it is possible to set a maximum and minimum limit either under the Administration program or by setting the values in the INI file. Another option is to have detection reports written to the system error log (SYS$LOG.ERR).

The Administration program has a separate facility to help define the destination of various reports depending on requirements. Details of infected files, scan summaries or scan progress can be shown on the *CSAV* administration screen and/or log file. Scan summaries can also be displayed on the console, while infection details can be reported to AlertTrack and the console as well as both the *CSAV* screen and the log file. When working with multiple servers, it is possible to define a master log server as a focal point for all the reports.

Alert Management and Updates

Alert management for workstation infections is handled separately using an additional NLM (AlertTrack Lite). This needs to be installed only on a single server and can be loaded separately at a later date. It provides the facility to send warning messages via various communication channels – Pager, Alpha-numeric Pager, MHS Mail, Pegasus Mail, SNMP, Broadcast Messages and FaxWare. This is provided simply by installing the appropriate workstation version of *Command AntiVirus* on the workstation.

There is a software deployment option which allows files to be updated on selected servers running *CSAV* within a domain. Two choices are offered. One deploys the *CSAV for NetWare* files and the other can deploy selected files from a defined list. This list could include the files for the workstation anti-virus software, which then could be pushed down to the client machines as needed.

Detection Results

The scanner was tested against the four *VB* test-sets – In the Wild File, Macro, Polymorphic and Standard – see the summary box for details. The virus signature list tested was identified as SCN 2.28 with Macro definitions updated to MDEF 980203.

Although the scanner had been set to delete infected files, the default option of copying files to the quarantine directory before deletion was in operation and made copies of all files which were detected as infected or suspicious. Despite achieving 100% against the Macro test-set, the other results were poor. Thirty samples were missed from the In the Wild File test-set (four of Anxiety.6093, eighteen of Morphine.3500 and eight of Spanska.4250) – these were all new to the WildList in December 1997.

While 79 samples were missed in the Standard test-set, the worst results were observed against the Polymorphics, with *CSAV* barely achieving 50% success. [*In fact, lower if the weighting algorithm used in the comparative reviews is applied. Ed.*] Of greatest concern here was the near-total failure to detect the Spanska.4250 replicants – a widely distributed In the Wild polymorph.

Real-time Scanning Overhead

To determine the impact of the real-time scanner on the server's performance, the following test was executed. Sixty-three files totalling 4,641,722 bytes (EXE files from SYS:PUBLIC) were copied from one server directory to another using *Novell's* NCOPY, which keeps the data transfer within the server itself, minimizing network effects. Various combinations of settings were used, including running the on-demand scanner concurrently with on-access scanning. The directories used for the source and target were excluded from the on-demand scan to avoid the risk of a file being scanned while waiting to be copied.

As mentioned earlier, there is a delay with real-time scanning to ease the load on the server. In order to test the real-time scan sensibly, it was necessary to introduce an extra routine which performed an open and close on each file copied to the target directory. Due to the different processes which occur within the server, the time tests were run ten times for each setting and an average taken. The utilization was left at the default of 40% and the number of buffers left at their default of 20.

The test conditions were:

- NLM not loaded. This establishes the baseline time for copying the files on the server.
- NLM loaded, Open = No, Close = No, and Scan = No. This tests the impact of the scanner in its quiescent state with no real-time or immediate scan in progress.
- NLM loaded, Open = Yes, Close = No, and Scan = No. This shows the overhead when reading incoming files.
- NLM loaded, Open = No, Close = Yes, and Scan = No. This shows the overhead when writing outgoing files.
- NLM loaded, Open = Yes, Close = Yes, and Scan = No. This shows the overhead when having both read and write scans in effect.
- NLM loaded, Open = Yes, Close = Yes, and 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.

See the summary for the detailed results. The timing tests were repeated with AlertTrack Lite loaded. No interesting variations were noticed in those results.

The initial impact of loading the scanner software is minimal. However, it begins to take effect when one of the real-time scans is selected. The impact of the real-time scanner does not vary a great deal between different selections and therefore checking when both opening and closing files is an option. The overhead when running AlertTrack was negligible and within the accepted variability of timing results. The residual overhead, when the NLM is unloaded, is minimal and is due to CLIB and Streams NLMs remaining loaded on the server.

Conclusion

Command AntiVirus for NetWare is going through a period of transition as the developers make efforts to customize the product as their own. Consequently, there is still inconsistency between product name and file/directory names. No doubt in due course all references to *F-PROT* will be replaced by the appropriate *CSAV* nomenclature and documentation. Unfortunately there are a number of more pressing problems which need to be addressed.

Firstly, the real-time statistics display on the main screen does not appear to be working at all. Secondly, although macro detection is excellent, the detection rate in the other areas is hardly inspiring. Having said all that, the configuration options are good, and I feel it is always a good thing to have the ability to control activity from both console and workstation. Furthermore, the extra option of having a central INI file which allows the standard settings to be propagated onto other servers eases deployment issues. The detection engine needs sorting out, but overall, the product holds a lot of promise for the future.

Command AntiVirus for NetWare v4.0

Detection Results

Test-set	Viruses Detected	Score
ItW File	621/651	95.4%
Standard	798/887	90.0%
Macro	745/745	100.0%
Polymorphic	7071/13500	52.4%

Overhead of On-access Scanning:

Time in seconds to copy 63 EXE files (4.6 MB). Each test was repeated ten times and an average taken.

	Time	Overhead
NLM not loaded	7.1	–
NLM loaded, inactive	7.7	8.5%
– + enabled +scan incoming	12.8	80.3%
– + – + scan outgoing	13.1	84.5%
– + – + scan both	13.0	83.1%
– + – + – + immediate scan	14.6	105.6%
NLM unloaded	7.2	1.4%

Technical Details

Product: *Command AntiVirus for NetWare v.4.0.*

Developer: *Command Software Systems Ltd*, Millbank Tower, London, SW1 4PQ, UK. Tel +44 171 931 9301, fax +44 171 931 9302, email sales@command.co.uk, WWW http://www.commandcom.com/.

Price: Single sever £360. Volume discounts are available.

Hardware Used: Server: *Compaq* Prolinea 590, 80 MB of RAM, 2 GB hard disk, running *NetWare 3.12*. Workstation: *Compaq* Deskpro XE 466, 16 MB of RAM, 207 MB hard disk, running *Windows 95*.

[1]Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NT/199803/test_sets.html.

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

The ICSA's conference, *IVPC '98: Protecting the Workplace of the Future*, will take place at Lake Buena Vista, Florida from 28–29 April 1998. For the first time it will run concurrently with a new event. *Remote Access: Building and Managing the Workplace of the Future* is to be presented by *GartnerGroup*. For more information about registration discounts and availability contact Ashley Pearce; Tel +1 203 316 6757, or email ashley.pearce@gartner.com.

***Trend Micro Inc* announces the release of *ScanMail* and *InterScan VirusWall* for *Microsoft Exchange* which are now available for *Digital Alpha Server* systems running *Windows NT*.** Prices starts at £955 for 50 users. *ScanMail* was recently chosen by *Hewlett Packard* to protect its *OpenMail* facility. For further details on these products, email trend@peapod.co.uk.

The eighth annual NetSec conference will take place at the Hyatt Regency in San Antonio, Texas from 15–17 June 1998. *NetSec '98: Network Security in the Open Environment* focuses exclusively on the security issues, problems and solutions facing networked environments. There are exhibitions throughout the programme and one and two-day seminars planned for before and after the conference. Contact *CSI* for details; Tel +1 415 905 2626, fax +1 415 905 2218, email csi@mfi.com or visit the web site at http://www.gocsi.com/.

Raptor Systems* announces *Eagle 5.0, the latest addition to the *Eagle* family of firewalls. Using a new data 'fastpath', this version can support in excess of 45 MB/s of mixed data throughput. Prices range from $3,995 to $15,000. *Raptor* is moving to a native *NT* GUI in the new firewall. Named *Hawk 6.0*, it will be offered as a free upgrade to *EagleNT 5.0* customers when it ships later in 1998.

***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 informaton can be found at http://www.infosec. co.uk/.

In early March, *Integralis Technology Ltd* ships ***MIMEsweeper 3.2 for Microsoft Exchange* versions 5.0 and 5.5.** More information can be found at http://www.mimesweeper.com/.

The North America Computer Audit, Control and Security (CACS) conference will be held at the Hyatt Regency O'Hare in Rosemont, Chicago from 26–30 April 1998. Subjects covered include disaster recovery and Internet security. Contact the Information Systems Audit and Control Association for information; email conference@isaca.org.

***Integralis Technology Ltd* and *Trend Micro Inc* have reached a settlement of the patent lawsuit between them.** The case, pending for seven months in a US District Court in Washington, has been dropped as part of the resulting mutual agreement. The two companies have also signed a cross-licence agreement sharing some of each other's technology and patents.

***Network Associates* has launched *VirusScan 3.0* for Macintosh.** As well as all the usual features (real-time and on-demand scanning with *McAfee's* Hunter technology), a pre-configuration 'wizard' customizes *VirusScan* according to how often the user downloads files from the Internet, friends or floppies. Virus Alerts are via Claris E-Mailer and Eudora. *VirusScan 3.0* costs $29.95, and free 30-day evaluations are available. For more information refer to the company's web page at http://www.networkassociates.com/.

The Audit Commission's February 1998 update is entitled Ghost in the Machine: Analysis of IT Fraud and Abuse. New research conducted in the form of a survey of 900 public and private sector companies reveals that the UK currently spends £26 billion on IT and that computer fraud and abuse affects 46% of businesses – up from 36% in 1994. Computer viruses were the most prevalent form of IT abuse reported, with the cost to organizations of each virus alert rising from £1000 per incident in 1994 to over £1700 in 1997.

After three years of technical cooperation, *Norman* is to acquire *ThunderByte*. *ThunderByte* Headquarters, in Wijchen, the Netherlands, now known as *ESaSS BV*, is to be renamed *Norman Data Defense Systems BV*. All *ThunderByte* security products will be incorporated into the *Norman* product range. Gunnel Wullstein, President of *Norman Data Defense Systems* believes 'In the future, only the strong technical players will survive. Good marketing is not enough.' Contact Harald Zeeman for details; Tel +31 24 6488555, or email zeeman@norman.nl.