ISSN 0956-9979 SEPTEMBER 1997

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

IN THIS ISSUE:

• **Memorial stone:** This month's virus analyses focus on a a DOS COM/EXE and *Windows 95* virus with an interesting manner of going resident, and a DOS virus that goes zombie. Read about them from p.6.

• **A scan for all seasons:** We test the mettle of eighteen of the latest anti-virus products for *NT* from major suppliers. Our comprehensive results could save you time and money. Compare the scores for yourself from p.10.

• **Read all about it!** Check out the latest from *Dr Solomon's* and *Iris*. Our two product reviews look at *NetWare*- and *Windows 95*-based software respectively. Catch up on developments, beginning on p.18.

CONTENTS

EDITORIAL

Trying Times

For the last month or so I've been fairly deeply embroiled in getting the *NT* comparative done. Interesting at times, boring at others (relentlessly feeding 91 infected diskettes into a PC, one after the other, product after product is not my idea of fun!), puzzling even (can loading a file-system service *really* improve *NT's* overall disk system throughput? – apparently, yes), and so on.

I've been a bit too busy really to notice much else in the industry though. At least, until I had to write this column.

One billion dollars! Difficult to miss that.

As I write this we still have not heard or seen any official response from *Symantec* to *McAfee's* latest shot in their 'let's make our lawyers even richer' contest. Many in the industry are amazed. In fact, to many it seems almost to be a game. But maybe that is a reasonable description of what most people outside the US see as its overly litigious system. American friends explain that if you do not counter-sue there is 'implicit guilt', and hence the escalating spirals of suit and counter-suit we associate with the US corporate legal battles.

I am, of course, focusing on the process here, not the claims themselves. In a nutshell, earlier this year, *Symantec* claimed that *McAfee's* crash-protection software, *PC Medic*, contained code identical to the most crucial piece of 'resuscitation' code in *Symantec's Norton CrashGuard*. *Symantec* later claimed that, following code examination by an independent expert in a court-ordered discovery process, more of their code was found in other *McAfee* products. *McAfee* acknowledged that approximately one hundred lines of code in the *VirusScan* code-tree is also in *Norton Antivirus'* code-tree, but claimed they obtained this code from a public domain source. Further, *McAfee* said this code was never compiled into a shipping product, as it was inadequate to their needs, and they eventually wrote their own replacement code.

This latter disclosure was met by *Symantec* with a press release titled 'McAfee confirms that VirusScan contains misappropriated Symantec code'. Now I'm no literary scholar, but that must be slightly more than a stretch! In light of this, I suppose it is hardly surprising that *McAfee* filed its $1 billion defamation and trade libel suit against *Symantec*.

Given the implicit guilt of their not responding, one can only wonder at what *Symantec* can do to top a $1 billion damages claim. I guess this could go on and on…

Elsewhere this last month, an anti-virus company was seen to be soliciting viruses on its web pages, offering monetary rewards to those who sent new viruses that the company's analysts found most challenging. This 'contest' has subsequently been portrayed as a mechanism for obtaining samples of viruses the vendor had been unable to come by from other sources. Unfortunately for the vendor, this seemed to much of the rest of the industry like soliciting from the virus writers. The competition was withdrawn following a suggestion by a professional body, of which the company is a member, that the contest was in breach of its membership code of ethics.

In Israel, where the vendor is based, it may well be reasonable to assume that requesting samples of existing viruses will result in only existing viruses being sent. For better or worse, most of the rest of the world seems to think otherwise, and sees events like this as encouraging the virus writers, which is something the anti-virus industry does not wish to do.

To this end, *Virus Bulletin* has invited a reformed virus writer to the VB'97 conference in San Francisco. Mike Ellison, formerly known as Black Wolf and Stormbringer, will present his views on why, three years after writing his last virus, he should be considered employable. He occupies the rather anomalous position of someone who has the programming skills and background that so many anti-virus developers complain are in short supply, but who, because of his past, is unlikely to find employment in that industry sector. This should prove to be a most interesting session!

NEWS

Defusing the Situation

The Middlesex-based computer security firm *Portcullis* recently launched *Defuse Enterprise*. Based on their year-old *Defuse Server*, this latest version offers macro protection for *Word 6* and *Word 7*. Loaded completely within *Word for Windows*, *Defuse Enterprise* interprets every line of WordBasic code (the language of macros), and on finding any malicious code, strips the macro from the document. The Administration PC then receives a full analysis along with the macro, and users can only access clean documents.

Portcullis' technical director Paul Docherty stresses the convenience and efficiency of *Defuse Enterprise*. He claims that rather than being just another anti-virus product, it is a 'network security tool, a powerful source of protection against a number of different threats. They include: letterbombs, firewall-hoppers, covert mail conduits, eavesdroppers, password grabbers and data kidnappers' ▮

The Suite Smell of Success

The *VirusScan Security Suite (VSS)* is released to corporate and home PC users this month by *McAfee*, which claims that it 'pulls together every security component necessary for maintaining complete desktop protection.' The *VSS* combines a number of modules including *QuickBackup*, *PCCryptic*, *PC Medic*, *NetCrypto*, *PCFirewall*, *VirusScan*, *WebScanX*, and *SecureCast*. The resulting protection capabilities range from eradicating viruses, eliminating lost data and time due to security breaches and encrypting or authenticating sensitive information, to automatically backing up data and downloading anti-virus updates.

The *VirusScan* module within the suite offers a high level of detection using Hunter technology, as well as automatic elimination of viruses from the Internet, Intranet, macros, email, and network files. It also provides protection for *Office 95* and *Office 97*, and can boast the top detection rates for both *Word* and *Excel* macro viruses. When a *Windows 95* computer is idle, the new *ScreenScan* utility automatically launches a virus scan. *McAfee* is the first anti-virus company to offer protection from ActiveX and Java Applets. These applications are downloaded from the web, often without the user's knowledge. *WebScanX* keeps an updated record of malicious Java and ActiveX programs and blocks them from damaging sensitive data.

UK marketing manager Caroline Kuipers is confident of the product's success: '*VSS* provides users with a solution that makes their whole computing environment safer and more secure, versus just a quick virus fix. *VSS* is the broadest computer security solution available today, at a highly competitive price' ▮

Prevalence Table – July 1997

Virus	Type	Incidents	Reports
CAP	Macro	85	24.5
Laroux	Macro	37	10.7
Concept	Macro	25	7.2
Wazzu	Macro	20	5.8
NPad	Macro	18	5.2
AntiCMOS	Boot	15	4.3
Temple	Macro	12	3.5
AntiEXE	Boot	10	2.9
Form	Boot	9	2.6
Switcher	Macro	6	1.7
Parity Boot	Boot	5	1.4
Since	Macro	4	1.2
Stoned	Boot	4	1.2
Appder.A	Macro	3	0.9
Delta	Macro	3	0.9
Demon.A	Macro	3	0.9
DZT	Macro	3	0.9
LBB Stealth	File	3	0.9
Niceday.A	Macro	3	0.9
Toten	Macro	3	0.9
Dodgy	Boot	2	0.6
Havoc	File	2	0.6
Crawen.8306	File	2	0.6
Kompu	Macro	2	0.6
Monkey	Boot	2	0.6
NOP.A	Macro	2	0.6
NYB	Boot	2	0.6
Pesan	Macro	2	0.6
Rapi	Macro	2	0.6
Ripper	Boot	2	0.6
Showoff	Macro	2	0.6
Wllop	Boot	2	0.6
Others		52	15.0
Total		347	100

Alarm, Amse, Apadana.1500.B, Baboon, BadSec.3248, Bandung, Bleah, Boring, Cascade-1701, Date.B, DLH.308, DMV.E, DSME, Gable.A, Helper.A, Hiac, HLL.5850.D, HLL.5850.E, HLL.ow.6028, HLL.ow.6736, Icrack, Irish, Jerusalem.AN, Junkie, Lavot, Leandro, Matura.1626, MacGyver, Milky, Minimal.C, Natas, NDTC, Nightshade.A, Nuker.A, Ocean.1021, Ordure, Paycheck, Peru, Quandary, Rotceh.B, RP, Schumann.B, Skim.1455, SlovakDictator, Stoned.Angelina, Tentacle, Twolines, Ulcer.1129, VCL.652.B, Wanderer, and WelcomB.

VIRUS BULLETIN **©1997 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /97/$0.00+2.50**

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

Type Codes

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

Anomaly.277

CN: An appending, 277-byte, direct infector infecting three files at a time. It contains the texts 'VoFcA', 'Deimos Anomally', and '*.CoM'.

```
Anomaly.277         E858 00B4 3FB9 1501 8D96 0301 FEC4 CD21 B801 573E 8B8E 3102
```

Antiskola.2111

CER: An appending, 2111-byte virus, from the Czech Republic containing the text 'TURBO.EXE TPX.EXECOMMAND.COM'. The payload that may trigger when an infected program is run, generates a sound through the speaker, and displays the usually encrypted message: 'Dobry den,predstavuje se Vam virus AntiSkola.Tento virus byl napsan pro demonstraci idealniho preziti viru ve skolnim prostredi. Doufam, ze se Vam bude libit. Moje podekovani patri zejmena : Firme Borland International Inc. za TurboAssembler a TurboDebugger Skole za to,ze mi umoznila nerusene programovat Firme Microsoft za "operacni system" MS-DOS,ktery byl koncipovan primo pro viry.Na prikladu WINDOWS 95 je jasne videt,ze se stale teto filozofie nevzavaji.Mozna by si meli neco precist o protected modu a preemtivnim multitaskingu. At zije SOSE v Brne na Obranske !!'

```
Antiskola.2111      8A44 04A2 0201 B891 F6CD 213D 5953 7478 8CC0 488E C026 803E
```

ATB.1522

CER: A stealth, appending, 1522-byte virus containing the texts 'Welcom jion in A block troop of Computer' and 'This virus made by ATB(1991/4)'. Infected files have their time-stamps set to 60 seconds.

```
ATB.1522            B9F2 0590 B440 CD21 B43E CD21 BAE1 008B 0E1C 03F6 C101 7405
```

BitAddict.432

CR: An appending, 432-byte virus containing the texts: 'The Bit Addict says: "You have a good taste for hard disks, it was delicious !!!"' and 'This virus is made by the Bit Addict !!!'. After infecting 100 programs the virus overwrites the first 100 sectors on drives C and D.

```
BitAddict.432       8CC8 8ED8 B800 40B9 B001 33D2 CD21 721B B800 4233 C933 D2CD
```

Bomber.1347

CR: An encrypted, appending, 1347-byte virus, containing the texts '(c) Copyright by Beast.', '(c) Stealth Group Bishkek.', '(c) Stealth Group World Wide.', 'Infection by Beast. v0.91', 'Stealth Group World Wide.', and '[Bomber v1.0] by Beast. Stealth Group World Wide.'. When an infected file is executed, the virus gains control through a series of direct and indirect jumps (e.g. PUSH AX, RET) spread across the host program (similar to the Commander Bomber virus).

```
Bomber.1347         7402 CD20 B8E0 E0CD 210C 0074 02CD 20E4 400A C075 02CD 2058
```

Dustbin.292

CN: An appending, 292-byte, direct infector containing the texts '*.COM', '[TAD2A] The Atomic Dustbin 2A - Just Shake Your Rump!', and 'Fail on INT 24 .. NOT!!'. All infected files have the word 4C4Dh ('ML') at offset 0003h.

```
Dustbin.292         8907 5BB4 40B9 2401 8D96 0501 CD21 B800 4233 C933 D2CD 21B4
```

Exorcist.272

CN: An appending, 272-byte, direct infector containing the texts '????????COM', '*.COM', and 'THe EXoRCiST'.

```
Exorcist.272        B440 8D96 0201 B910 01CD 21B4 3ECD 2181 3E00 010E 1F75 04B4
```

Gigi.1318

CR: An encrypted, appending, 1318-byte virus containing the texts 'SUCKER', '.COM', 'VSAFE', 'COMMAND', and 'WIN'.

```
Gigi.1318           FABE 0001 B937 0033 D2AC 32E4 03D0 8AD8 F6E3 03D0 E2F3 81FA
```

Gigi.1465

CR: An encrypted, appending, 1465-byte virus containing the texts 'Gigi Euristicu' v1.0 * RoMaNiA|Only COM infector but a new generation is comeing ...|Copyright [C] 1996-97 Elecktronick RAT & Pink Phanter |Special thanks to GikuABS (Ps!ko) |Who's General Failure and what's he doing on your HD ?', 'SUCKER', 'Rabbit', '.COM', 'VSAFE', 'COMMAND', and 'WIN'.

```
Gigi.1465           FABE 0001 B910 0033 D2AC 32E4 03D0 8AD8 F6E3 03D0 E2F3 81FA
```

Gly.1182

CR: A stealth, appending, 1182-byte virus containing the text 'G L Y Serial Number:'. Infected files have their time-stamps set to 24 or 56 seconds.

```
Gly.1182            80FC 4F74 493D AAAA 7504 9DF7 D0CF 9D2E FF2E 7E04 9C2E FF1E
```

HeadHog.555 **CR:** A stealth, appending, 555-byte virus containing the text 'This is HeadHog v1.1 Created by -== Raver ==- 1997'. Infected files have their time-stamps set to 2:08:34.

```
HeadHog.555     B440 8B1E F902 BA03 01B9 2B02 CDBB 33C9 33D2 8B1E F902 B800
```

Henon.429 **CN:** An overwriting, 429-byte, direct infector containing the texts '*.COM', '????????COM' and '*DeViANT MiND*'. The virus overwrites the last 429 bytes of host programs.

```
Henon.429       81EA A601 CD21 B440 8D96 0701 B9A6 01CD 21B8 0157 3E8B 8E51
```

Henon.448 **CN:** An encrypted, appending, 448-byte, direct infector containing the encrypted texts '*.COM' and '????????COM', and the plain-text string '*DeViANT MiND'.

```
Henon.448       B96A 018A A6B9 0247 8A05 32C4 8805 E2F7 33F6 5E81 FEFE 0074
```

Henon.526 **CN:** An overwriting, 526-byte, direct infector containing the encrypted texts 'Program too big to fit in memory', 'ComKiller has rectified your .com file overpopulation crisis!', and '*DeViANT MiND'.

```
Henon.526       E854 FFB4 408D 9607 01B9 0E02 CD21 E846 FFB8 0157 3E8B 8E97
```

Henon.547 **CN:** An encrypted, appending, 547-byte, direct infector containing the texts '????????COM', '*.COM', and '*DeViANT MiND'.

```
Henon.547       B9CD 018A A61C 0347 8A05 32C4 8805 E2F7 33F6 5E81 FEFE 0074
```

Henon.918 **EN:** An encrypted, appending, 918-byte, direct infector containing the texts '*.EXE', '????????EXE', 'Relax, open your mind, a low-life is in control.', 'Hit a key, butthead…', and '*DeViANT MiND*'.

```
Henon.918       BE72 01B8 4403 D1E8 8BC8 8B96 B804 4747 8B05 33C2 8905 E2F6
```

HongKang.1904 **CER:** An appending, 1904-byte virus containing the encrypted text, displayed on 7 April, 'Celebrate HongKang return to CHINA 1997 !'. Infected files have their time-stamps set to 60 or 62 seconds.

```
HongKang.1904   B8FF FFCD 213D 9719 7503 E9C4 00B8 0000 8ED8 BFFE 0481 3D97
```

IVP.2385 **CEN:** An encrypted, appending, 2385-byte virus containing the text 'NeonSniper', 'VoFcA', '*.com', and '*.exe'. The virus displays a rough sketch of a sports car and the message 'Hi.' Infected files have the word 4D4Dh ('MM') at offset 0003h (COM) and offset 0010h (EXE).

```
IVP.2385        8D9C 1A01 B925 092E 8A27 2E32 A455 0A2E 8827 43E2 F2C3
```

Jessica.1345 **CER:** An appending, 1345-byte virus containing the text 'Dear Jessica: This is to commemorate our pure and deep friendship which began in R405,PUDY,1992. My wanderlust comes from the love for freedom... Wanderer V1.1 NT' and the encrypted string 'CHKLIST.MS'. Infected files have their time-stamps set to 56, 58, 60 or 62 seconds.

```
Jessica.1345    2EFF 2E07 019C 3DEE EE75 05B8 3412 9DCF 5053 5152 061E 5756
```

Jorgito.721 **ER:** An appending, 721-byte virus, containing the encrypted text 'Jorgitø Was Here Córdoba Argentina', displayed on 14 March. Infected files have the word 524Ah ('JR') at offset 0012h.

```
Jorgito.721     BBD7 F993 CD21 3D83 7874 72BB 4154 438B C305 FE75 CD2F 9380
```

Konrad.999 **CR:** An encrypted, appending, 999-byte virus containing the texts '!ZuSe by DiGiTAL', '*.COM', 'by DiGiTAL [TECHNO]logies', 'Name: KoNrAd ZuSe 1.0ß ORiGiN: Ost-Berlin (FRG) Creator: -=-DiGiTAL -=-Size: 999 bytes/501 bytes last UpDate: 04-28-93', 'not resident infects COM-files only uses SeLf-EnCrYpTiOn RuN-TiMe oPeRaTiOon', and 'Grz2: ThE GuYz FrOm ThE FeZ, !TWIN, SyNeC, RoY, WaNgLeR 'n' all –=≡(*) TELEKOMiKER (*)≡=– (kotz,brech,ätz,krepel,übergib...'

```
Konrad.999      E8DC FFB4 40B9 E303 8D96 0801 CD21 E8CE FFC3
```

LJF.1098 **CER:** An appending,1098-byte virus containing the text (at the end of infected files) '(C) LJF. 96.6.1'.

```
LJF.1098        B855 FFCD 213D AA55 746D 2681 2E02 00C0 0026 A102 008C C149
```

Mipt.748 **CER:** An appending, 748-byte virus containing the text '(C)Terminator,MIPT(75)'. Infected files have their time-stamps set to 30 seconds.

```
Mipt.748        B4FE CD21 80FC 0074 4306 1E8C DB4B 8EDB 832E 0300 3983 2E12
```

Ominous.1846 **CER:** An encrypted, appending, 1846-byte virus containing the texts 'COMMAND' and 'Welcome to Scorpion Virus Copyright (C) '. Infected files have their time-stamps set to 58 seconds.

```
Ominous.1846    0E1F BE?? ??B9 2307 2E8A 0434 ??2E 8804 46E2 F5??
```

PS-MPC.289 **CN:** An appending, 289-byte, direct infector containing the text 'This is [ß] virus , non encrypted virusFrom Doctor Matrix, ItalyBased on PS-MPC*.com'.

```
PS-MPC.289      B002 E830 00B4 40B9 2101 8D96 0301 CD21 B801 578B 8E3C 028B
```

Roe.753 **CER:** An appending, 753-byte virus containing the text 'roetvir_E5'. The virus re-infects already infected files. The payload triggers in late December (28–31), generating a series of 255 beeps.

```
Roe.753         B888 B1CD 21EB C374 2F8C C0EB C483 2E12 0040 90EB C88B F5B9
```

V.246 **CN:** An appending, 246-byte, fast, direct infector containing the texts '*.com' and 'COMMAND.COM'. Due to a bug, the virus re-infects already infected programs.

```
V.246           21B8 0242 33D2 33C9 CD21 B440 8BD5 B9F6 00CD 21B4 3ECD 21C3
```

WCA.275 **CEN**: An overwriting, 275-byte virus containing the text '\\/ar Cannibal Animal..', '*.CoM', '*.ExE', and 'Incorrect DOS version'.

```
WCA.275         E836 00E8 4100 B440 B913 01BA 0001 CD21 B801 572E 8B0E 9600
```

Wintermute.1052 **CER:** An encrypted, 1052-byte appender containing the text 'Apocalyptic by Wintermute/29ACOM'.

```
Wintermute.1052 0800 8A14 8AC2 C0C2 0480 F2F9 80C2 0288 144E E2EE C3B0 03C3
```

VIRUS ANALYSIS 1

Junkie Memorial?

Péter Ször
Data Fellows

Clinton Haines did not have time to change for the better. He was an active virus writer and he died a junkie. The VLAD virus writer group have dedicated Memorial.12314 to him.

There has been a healthy development in *Windows* virus writing thus far, but the list of infectors is still not long. Memorial infects DOS COM and EXE files, as well as Win32 PE (Portable Executable) files. The main format of the virus is a *Windows 95* VxD (Virtual Device Driver). It takes an interesting new direction in loading its memory-resident component.

The virus is unencrypted in DOS COM and EXE files, but infected PE files are encrypted with an oligomorphic routine. Moreover, the main virus body (the VxD image) is packed with a simple algorithm. There is already one virus which is encrypted in PE files (Win95.Mad), but Memorial is certainly the first *Windows 95* virus with oligomorphic properties – thus, we see the first steps towards *Windows 95* polymorphism.

Memorial is also an effective retro-virus. It manipulates the registry to disable several anti-virus programs. Fortunately, the virus has a few serious bugs which can slow its spread. Despite this, Memorial.12413 has been reported to be in the wild in Sweden and Norway.

Running an Infected COM File

Windows 95 virus writers appreciate that people are still exchanging more DOS programs than *Windows 95* ones. This is a big problem for viruses; they simply cannot spread very far by infecting only *Windows 95* programs. Memorial addresses this by also targeting DOS executables, which then function as droppers of the main VxD module.

If *Windows* is running when an infected COM file is executed, the virus simply executes the host program. If *Windows* is not running, Memorial makes its 'Are you there?' call – Int 2Fh, AX=0h. If AX=4AB3h is returned, the virus assumes it is already active in memory and passes control to the host. Otherwise, it creates C:\CLINT.VXD with the hidden attribute, and starts to write into it.

Initially, the writing routine looked to me like an anti-heuristic function. That is not its aim, however. The main body of the virus is packed to 7508 bytes and this function is supposed to unpack it. The algorithm is very simple, but effective. VxD files are in LE (Linear Executable) format, and their structure contains many zeros. The full VxD is packed to 7508 bytes, and grows to 12413 bytes after unpacking. When CLINT.VXD is ready, Memorial copies a piece of code from its body into the Interrupt Vector Table at 0:200 and hooks Int 2Fh (Multiplex Interrupt). So, while the virus is not troubled with memory allocation, it is incompatible with some applications.

Aside from answering the 'Are you there?' call, the Int 2Fh handler waits for AX=1605h. This notifies DOS device drivers and TSRs that standard- or 386 enhanced-mode *Windows* is starting.

When Memorial receives the *Windows* initialization notification, it tries to open C:\CLINT.VXD to check for its existence. If this succeeds, it initializes the appropriate data structures to direct *Windows* to load C:\CLINT.VXD. Thus, the virus uses a documented way to ensure its resident part is loaded by *Windows*. This is more elegant than modifying the SYSTEM.INI file, and more successful.

Running an Infected PE EXE

On executing an infected PE file, the virus decrypts itself. C:\CLINT.VXD is dropped here, too. In the case of DOS infections, the dropper function takes 275 bytes of additional code at the virus entry point. In PE files the dropper is in 32-bit code and is more complex, so this code is longer – 1360 bytes. This function includes Memorial's activation routine and is also supposed to load the VxD.

Memorial works out the entry point, in memory, of the GetModuleHandleA function. It does this with a real hack: searching internal *Windows 95* structures. This makes subsequent PE infection easier. The virus need not add any entries to the Imported Names table, thus removing the need for a complicated patch function.

Next, it calculates the entry point of GetProcAddress with the same trick, before using GetModuleHandleA to get the handle of the KERNEL32 module. By manipulating this handle, Memorial is able to call GetProcAddress to find and save addresses for the CreateFileA, WriteFile, ReadFile, SetFilePointer, CloseHandle, GetLocalTime and LocalAlloc procedures. After this, Memorial is provided with USER32's handle by the same manipulation of GetModuleHandleA, and saves the address of the MessageBox procedure through further use of GetProcAddress.

The virus then calls GetLocalTime to check the date – if it is 10 April the virus activates and displays a message box. Otherwise, it checks whether \\.\CLINT is running. If so, the host program is executed. If not, \\.\C:\CLINT.VXD is created as a normal file using CreateFileA, and if successful, Memorial allocates memory for unpacking the virus body by calling the LocalAlloc procedure. It unpacks the VxD code to this buffer, then writes the resulting 12413 bytes into CLINT.VXD with the WriteFile function, before

closing the file with CloseHandle. The CreateFileA procedure then executes the VxD, and Memorial finally starts the host program.

Running an Infected DOS EXE

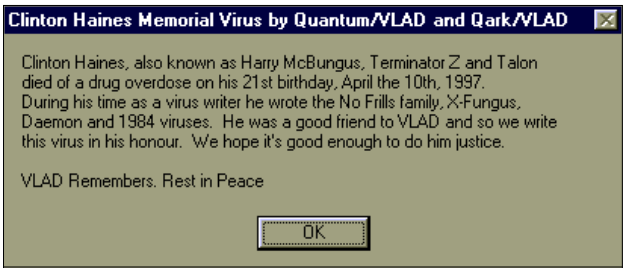
When an infected EXE file is run, the same unpacking code as in COM files takes control from the virus entry point. However, because of a major bug in the DOS EXE infection code, this function writes endlessly to C:\CLINT.VXD. Memorial uses an invalid pointer and a bad virus size parameter during EXE infection. Instead of writing the packed VxD code, it writes the unpacked copy. The dropper code 'extracts' an already unpacked VxD image. The extractor code writes megabytes to C:\CLINT.VXD, until it fills all available hard drive space, but even then, control does not return to DOS. The huge C:\CLINT.VXD can be located by pressing Ctrl-C during this operation or restarting the machine. Thus, Memorial can be classified as 'intended' in DOS EXE files. Fortunately, it is detectable and disinfectible in these cases.

VxD Initialization (IFS API hook)

CLINT.VXD's message handler waits for four control messages. In response to W32_DEVICEIOCONTROL it returns 00h, as it does not want to communicate with other applications. When a SYS_DYNAMIC_DEVICE_EXIT message appears, Memorial returns 01h to disallow the unload request. In the case of INIT_COMPLETE and SYS_DYNAMIC_DEVICE_INIT messages, the virus executes its initialization procedure which hooks the DOS IFS (Installable File System) API.

Memorial disables many *Windows 95* anti-virus programs by deleting or changing registry settings. Several keys that start the resident or on-access anti-virus programs are deleted under '\System\CurrentControlSet\Services\Vxd'. It also removes similar keys from '\SOFTWARE\Microsoft\Windows\CurrentVersion\Run'. Several keys are also deleted from '\SOFTWARE\McAfee\ScreenScan' and '\SOFTWARE\Cybec\VET Antivirus for Win32\'. *Cybec's VET* is further targeted by setting its 'Scanning\Extension List' value to 'bin, dll, doc, drv, ovl, sys, dot', removing 'com', 'exe' and any user customizations.

The virus then clears the attributes on C:\CLINT.VXD. Subsequently, it opens the file, checks and saves its size, and allocates enough memory for both its unpacked and packed copies. Then it reads itself from the file to the main buffer, before closing the VxD file and deleting it. After this, Memorial packs the VxD code into the second buffer, and returns from its initialization routine.



Memorial's 'tribute' to Clinton Haines

COM Infection

When Memorial intercepts a file open call, it checks the extension, comparing it first to 'COM'. If there is a match, the virus finds and saves the attributes of the victim file and clears them, allowing infection of read-only, system and/or hidden files. After opening the victim, it reads the first four bytes from it. If offset 03h is 'Z', Memorial assumes the file is already infected. If not, it checks for 'MZ' and 'ZM' markers. If the victim is of COM structure, the size is also checked – it only infects COMs between 7168 and 51200 bytes long. Next, it reads the last five bytes of the program and checks whether they start with 'SN'. If so, the file is not infected. I can see no reason for this other than the inoculation of a certain PC – the virus writer's own?

The 275-byte DOS dropper code is appended to the victim together with the 7508-byte packed virus image. Finally, Memorial changes the first four bytes to a jump to the virus body plus a 'Z' marker and resets the attributes. Thus, in the case of COM infection, the virus is 7783 bytes.

DOS EXE Infection

If a target starts with 'MZ' or 'ZM', the virus checks the extension against '.EXE' and '.SCR'. On a match, it calls IFSMgr_Get_DOSTime to seed its random number generator. The virus must add a section name to the header of its PE targets, but as it is oligomorphic, it does not want this to be a constant name. Thus it mutates 'CLINTON', using an 8-bit XOR, to a 'garbage' string and calculates a check byte, saving it as the last character of the string. This byte is used as a self-recognition check. The virus mutates the section name during DOS EXE infection only. This makes the mutation rather slow (slow oligomorphism).

Memorial then reads four bytes from offset 3Ch – a pointer to the *Windows* executable header area. If this pointer is 0, the virus assumes that the file is a normal DOS EXE file. If the checksum field of the EXE header is 6666h, or if the IP field is 100h, the virus will not infect.

It increases the size of EXE files to the next paragraph boundary and adds the VxD dropper code (275 bytes) to the end of the file. Then comes the virus' biggest bug: it writes the unpacked VxD to the end of the file (12413 bytes). Thus, the virus size is 12688 bytes where the victim is a DOS EXE file. Finally, it modifies the executable's header to point to the virus entry point.

PE Infection

If the double word at the 3Ch offset is not zero, Memorial checks for the PE signature, before studying the file's read-only attribute. Then it reads the last section name from the

Image Header structure and calculates the check byte on the section name. If the checksum matches, Memorial does not infect. Otherwise, it modifies the PE header by adding the new virus section to it. Since Memorial is oligomorphic, it first mutates its 46-byte long decryptor (see below) for the beginning of its body. Then it encrypts the PE version of the VxD dropper (1360 bytes), adding the decryptor then the dropper code to the end of the victim (1406 bytes). Finally, it encrypts the packed VxD image and adds it to the end of the file (7508 bytes), prior to restoring the victim's file attributes and closing it.

Oligomorphic Engine

This engine is simple but effective – the basic decryptor consists of eleven 'blocks' of interchangeable code. There are a total of 96 possible combinations, complicating the detection of the virus in PE files.

Conclusion

Memorial is a complex virus. Its discovery suggests that polymorphic *Windows 95* viruses will appear in the near future. One wonders whether polymorphic mutation engines for *Windows 95* viruses will be far behind. It is time to implement new scanning engines for these strange beasts.

Memorial

Aliases: Win95.Memorial.12413

Type: Windows 95 PE, DOS COM, EXE infector. Uses VxD to 'stay resident'.

Self-recognition in Files: Offset 03h of COM files is 'Z', DOS EXE files have 6666h marker in the EXE header checksum field. In PE files, tests a checksum byte on the last entry in the section name table (see text).

Self-recognition in Memory: Cannot infect system memory twice under *Windows 95*. Int 2Fh, AX=0 returns AX=4AB3h under DOS.

Hex Pattern in COM, EXE, VxD Files and in Memory:

```
0BC0 7504 B8B3 4ACF 3D05 1674
05EA ???? ???? 9C2E FFIE 2D00
```

Hex Pattern in PE Files: Not possible.

Intercepts: Int 2Fh, AX=1605h (Windows Initialization Notification), ISF API hook OpenFile (IFSFN_OPEN).

Payload: Displays a message box on 10 April.

Removal: Under clean system conditions, recover infected files from a backup or replace from original sources.

VIRUS ANALYSIS 2

Search for a Heart of Stone

Snorre Fagerland
University of Bergen, Norway

StoneHeart.1490 contains some unusual tricks aswellas being quite picky about which files it will infect. It bears a strong similarity to the Nostardamus family, and could even be said to be a Nostardamus variant. It appears to have been written by the same author – Eternal Maverick of the Russian virus-authoring group 'Stealth Group World Wide' (where do they get these names from?).

Entry

On entry, the virus code first checks that the active PSP points to its own data segment. If not, it starts overwriting the current data or code segment with its own segment address in a loop, finally corrupting running code to a miserable end. This piece of code will probably never be run – it is an anti-heuristic trick, designed to foil scanners that rely heavily on heuristics, in particular *Dr Web*. Next it calls the DOS GetDateTime function (Int 21h, AH=2Ah), with BX=454Dh ('EM') as an installation check. If already resident, this call will return BX=4D45h ('ME').

Memory-residency – Part One

The virus makes itself memory-resident by shrinking the current memory block by 5E0h bytes. It does not create any new MCBs – this can cause memory blocks to drop out of the MCB chain and DOS to react badly (does 'Memory allocation error – system halted' ring a bell?). However, most of the time it will load as the last program in the MCB chain and set up a segment at the top of DOS memory. It then copies 1490 bytes into the new host segment.

At this stage StoneHeart performs a destructive action; it seeks out and truncates files matching C:\??????C?.???, D:\??????D?.??? and so on, going down the whole drive chain. This is aimed at *ADINF* checksum tables, but could affect other files. While this happens the DOS critical error handler (Int 24h) is disabled. Apart from being truncated, these files also have the system attribute set.

Night of the Undead

After its truncation spree, StoneHeart does something unusual, which I have only seen in the Nostardamus family. It goes 'zombie'. It does the digital version of dying, to be dug up later. This is an anti-monitoring trick, for most activity monitors keep very close track of memory and interrupt status during the execution of a program. If something happens after the program has terminated, the monitors often miss it.

To achieve this, StoneHeart saves the Int 22h terminate address at offset 0Ah in the PSP, and replaces it with a pointer to its own code. When the host program terminates, DOS will free memory, files and buffers associated with the program. Any activity monitors will kick in, find memory status unchanged and thus allow DOS finally to return execution to the address stored at 0Ah in the PSP.

Memory-residency – Part Two

On regaining control when the host terminates, StoneHeart uses standard DOS services to allocate a new segment covering 13Ch paragraphs (5056 bytes). It needs such a big memory space for its encryption buffer; and for disk I/O. If it cannot manage to do this, it just quits – this time it is really dead. On successful memory allocation, it marks the new memory block (probably in the newly-freed memory space of the host) as belonging to the BIOS, before hooking Int 21h directly from the vector table. It then jumps back to the original Int 22h terminate address, leaving a fully-working TSR.

The virus traps four DOS Int 21h functions; AH=4Bh (execute), AH=3Dh (open file), AH=43h (Get/Set file attributes), and AH=2Ah (GetDateTime).

The GetDateTime call is used only for StoneHeart's 'Are you there?' call. The real action takes place in the other functions, which have in common that they take a file name parameter in DS:DX. It seems that the author may have read Ralf Brown's INTLIST because of the use of the little-known multiplex function Int 2Fh AX=1211h to normalize the file name. You do not see that in use every day.

Picky, Picky…

StoneHeart only infects EXE files if the filename neither ends with the letter 'F' (e.g. ADINF.EXE) nor contains any digits. It also avoids infecting files starting with 'AID', 'AVP', 'PRO', 'SCA', 'EXT' or 'WEB'; files with the system attribute set; files smaller than 4096 bytes; files with an EXE header larger than 200h; or files larger than the file size field in the EXE header. On infection, the minutes field of the target's time-stamp is set to a multiple of eight and the seconds field is set to 30 – a variant of a trick first used by Frodo. Potential targets matching this are also not infected.

Another curiosity – StoneHeart will not infect if there is a write-protected diskette in the A: drive, which it determines by using direct drive controller manipulation. This happens even if the target executable is located on the hard drive.

Infection Process

When StoneHeart deems a file worthy of infection, it encrypts its own code and appends this to the file. It then adjusts the CS:IP pointer in the EXE header to the virus entry point. This is a standard approach. What is not so standard is that it encrypts the first 512 bytes of the original program code, deliberately making proper disinfection very difficult. The key is located inside the encrypted virus body. As this virus is not stealth it does not need to pad itself up to a fixed size like some of its Nostardamus cousins. The infective length change will thus vary from around 2080 to 2120 bytes, depending on decryptor size.

Polymorphism

All members of the Nostardamus family are polymorphic, employing the mutation engine EMME – Eternal Maverick Mutation Engine. EMME is a multi-level engine, meaning that the decryptors generated by this module are layered. The first decryptor decodes another decryptor etc, which will decrypt the virus. StoneHeart uses EMME_Small which is not multilayered, and is only about 530 bytes long, compared to EMME 3.0 at about 1000 bytes.

EMM_Small is a hybrid mutation engine, combining both tabular lookup and runtime-generated opcodes. It creates one- to four-byte garbage instructions, and generates decryptors with a length of 80 to 120 bytes.

Conclusion

Despite being a development from the Nostardamus family, StoneHeart does not perform direct format or system sector corruption, but does have a potentially destructive payload. It has also been designed to be difficult to disinfect without corrupting the host. Thus, Eternal Maverick seems to be continuing the tradition started with Nostardamus.3584.

StoneHeart.1490

Aliases:	EMME_Small.StoneHeart.1490
Type:	Resident, no stealth.
Infection:	EXE files, checks for EXE extension and both 'MZ' and 'ZM' in the header.
Self-recognition in Memory:	Interrupt 21h, AX=2Ah, BX=454Dh returns BX=4D45h.
Self-recognition in Files:	Time-stamp has minutes in multiples of 8 and the seconds value will be 30.
Hex Pattern in Files:	None possible.
Hex Pattern in Memory:	`B42A BB4D 45CD 2181 FB45 4D74 365E 5683 EE1F 06A1 0200 2D5E`
Intercepts:	Interrupt 21h, functions 3Dh, 43h, 4Bh for infection. Function 2Ah for installation check.
Removal:	Boot from a clean system disk, then replace infected files.

COMPARATIVE REVIEW

NT Promises

The last time we ran a *Windows NT* scanner comparative (*Virus Bulletin*, October 1996, p.8), we concentrated on *NT* as a server platform, on the grounds that, at the time, *NT* was most widely deployed as a server. How things change in a year! RAM is much cheaper, as are large hard drives and fast Pentium processors – all resources that have previously kept adoption of *NT* at a level somewhat lower than *Microsoft* desired. With these price reductions, however, *NT* is being much more widely deployed as a desktop operating system, and many companies which avoided the *Windows 95* 'interim' step are now moving to *NT en masse*.

Thus, the focus of this *NT* comparative review is squarely on *NT* as a desktop operating system. Many of the vendors represented in this review have separate products for use on *NT Server*, and if that is your interest, do not assume that performance on these tests relates directly to those products. Eighteen products were submitted for review, with active monitoring or on-access scanning a more common option than in last October's comparative review.

Testing

The same machine was used for all of the tests except for the boot sector detection tests, which were run in parallel to the file-scanning tests to reduce total testing time. Testing was done from the Administrator usercode on a standalone *Windows NT 4.0* workstation with Service Pack 1 installed. The workstation software was restored between each product test from a sector-level image backup. None of the products claimed to need any particular level of Service Pack, and as both SP2 and SP3 have been known to cause problems with some anti-virus programs, this seemed a reasonable compromise.

The test-sets used in this review are slightly updated from those used in the July DOS comparative, taking into account the changes from the May WildList. Thus the 'new' Macro test-set was used, along with the usual In the Wild File and Boot, Standard, and Polymorphic test-sets. The recent standard clean test-set was used for on-demand scanning time and on-access overhead tests.

When scanning the virus test-sets, the products' default settings were generally used, but, whenever possible, the 'delete infected files' option was enabled. If such an option was not available, the 'move infected files' option was used instead. On completion of a scan, the number of files deleted or moved from the virus test-set directories was compared with the number of viruses claimed to have been detected, and any anomalies accounted for (for example, some products will not delete files infected with viruses like Dir_II, which use the 'cluster attack' method). In the case of a couple of scanners, it was necessary to resort to checking log files to collate the detection results.

In the main speed tests, the scanners were run against a substantial collection of non-infected programs – after all, this is how they spend most of their working lives. No other programs were active during these tests, the scanner was the foreground application, and *NT's* scheduling was set to its default of 'Maximum boost for the foreground application'. This test doubles as a false positive test – no viruses should be reported here.

The Technical Details section at the end of this review contains more details and there is a WWW address for a document explaining the calculation scheme employed in recent *VB* comparative tests. The latter is essential reading in order to understand the detection percentages we report.

Resident Software

Twelve of the products reviewed provided some form of resident or on-access scanning capabilities. Time constraints precluded running the resident scanners through detection tests. The performance overhead introduced by these components is an important factor to consider, and was measured. In two cases we were unable to do so reliably – in one because the on-access sub-system kept shutting down during the tests, and in the other because of the variability of session-to-session performance and having to restart the machine for changes to the on-access scanner's configuration to take effect.

How to measure on-access scanner overhead is a tricky issue. A process similar to our server overhead tests was settled on. After setting the desired scanner configurations, all other programs were closed except a Command Prompt, and it was timed how long it took to copy a sub-directory of files (from our Clean test-set) to another sub-directory . These copies were repeated ten times and the average calculated for each combination of on-access settings. Before each set of copies, the disk cache was 'primed' by running a copy which was not timed. The overhead was then computed relative to a similar set of timings made when the on-access components were not loaded at all.

This is really a worst-case test. In 'normal' day-to-day use, workstation users probably seldom perform such intense executable file copies. Some of the results were daunting, in one case a 400% overhead was observed.

Presenting these results also poses a problem, due to the inherent performance variability mentioned above. To allow for this, the results have been normalized to a baseline copy time of twenty seconds with all reported test

	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil AVAST32	91	100.0	548	99.4	99.6	711	99.5	11500	88.5	774	100.0
Cheyenne InocuLAN	91	100.0	548	99.7	99.8	624	87.7	11482	86.4	764	98.6
Command F-PROT	91	100.0	544	98.1	98.8	695	96.8	7059	48.4	678	91.0
Cybec VET	91	100.0	548	99.4	99.6	700	97.9	12482	95.1	750	97.4
Data Fellows F-PROT	73	80.2	547	98.7	91.9	695	96.8	7050	50.3	684	91.6
Dr Solomon's AVTK	90	98.9	549	100.0	99.6	712	100.0	12938	97.7	774	100.0
EliaShim ViruSafe	89	97.8	543	99.4	98.8	607	85.0	11632	83.5	749	97.5
H+BEDV AntiVir/NT	65	71.4	507	91.3	83.9	650	90.4	9600	72.7	660	90.1
IBM AntiVirus	91	100.0	547	98.7	99.2	710	98.9	12500	96.2	773	99.7
Intel LANDesk Virus Protect	82	90.1	540	98.3	95.3	577	80.7	11382	85.9	743	97.2
Iris AntiVirus Plus	91	100.0	548	99.7	99.8	670	94.3	11483	87.4	766	98.9
Kami AVP	75	82.4	548	99.7	93.3	712	100.0	12499	95.2	755	98.8
McAfee VirusScan	91	100.0	549	100.0	100.0	712	100.0	12941	98.7	754	98.4
Norman ThunderByte Virus Control	75	82.4	549	100.0	93.5	712	100.0	12548	93.5	751	97.8
Norman Virus Control	91	100.0	549	100.0	100.0	709	99.6	11500	88.5	669	92.2
Sophos SWEEP	91	100.0	549	100.0	100.0	712	100.0	13000	100.0	772	99.7
Symantec Norton AntiVirus	91	100.0	548	99.7	99.8	699	97.9	11498	87.5	728	96.9
Trend Micro PC-cillin NT	87	95.6	543	99.0	97.7	692	97.3	11882	89.7	716	94.7

results scaled to this. Another problem is that of comparing apples and oranges – there are as many configuration options as there are scanners. For simplicity's sake we have loosely classified the on-access scan options as 'read-only', 'write-only' and 'read and write'. Some products give much more fine-grained control than this, whereas others have options labelled 'file open', 'file close' and so on. The most comparable configuration option is probably the 'read and write' one.

Remember when looking at the overhead results that these are for bulk copying of files that scanners will inspect – the overhead seen on other, more typical, computing operations is likely to be different. However, as the number and type of files that have to be scanned increase, one wonders how long this will remain true…

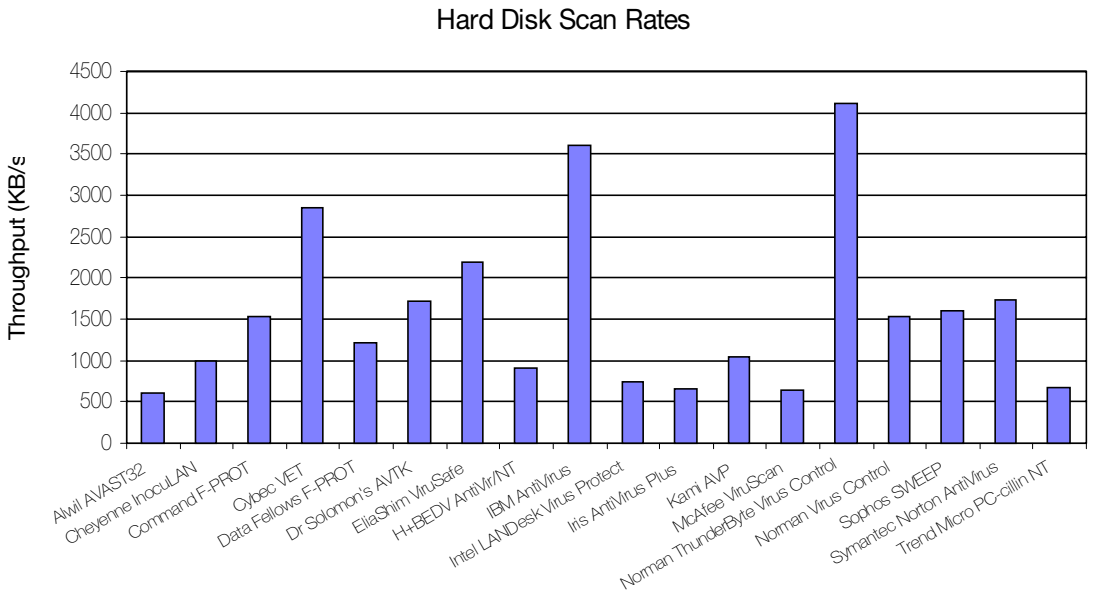
As the focus of this review is on *Windows NT* as a workstation operating system, it was not considered important to 'soak test' the scanners.

Alwil AVAST32 Build 354 25 June 1997

ItW Boot	100.0%	Macro	99.5%
ItW File	99.4%	Polymorphic	88.5%
ItW Overall	99.6%	Standard	100.0%

In the previous *NT* comparative, we noted that the Help files were in Czech – these have now been translated into English for the 'English version' of the product. The user interface has changed little.

A very good performance from *AVAST32* – perhaps not quite in the top league, but with 100% on the ItW Boot set, just one sample of the *Word 8* Wazzu.C macro virus stood between it and perfect scores on the ItW File and Macro test-sets. 100% on the Standard test-set is a pleasing score, but missing all 500 samples of each of Baran.4968, Cryptor.2582 and Mad.3544 viruses lowered its Polymorphic score considerably. These results are consistent with those of *Alwil's* scanners in our recent comparatives.



AVAST32 suffered one false positive against the Clean test-set. It is no speedster either, having the rather ignominious distinction of being the slowest scanner in this review, with a data-rate of 613 KB/s. As one of the products without an on-access scanner, there are no performance overheads to report. The developers justify omitting on-access scanning from their *NT* version, but including it in the *Windows 95* version, on the grounds that DOS file viruses are less likely to spread successfully under *NT*. That point is debatable itself, but overlooks the main reason for much of the current interest in on-access scanning – the increasing prevalence of macro viruses, and concerns about email attachments and Internet downloads.

Cheyenne InocuLAN v4.0 8 July 1997

ItW Boot	100.0%	Macro	87.7%
ItW File	99.7%	Polymorphic	86.4%
ItW Overall	99.8%	Standard	98.6%

A typically solid performance from *Cheyenne InocuLAN*, sitting around mid-pack on the detection tests and a little lower than this on the speed tests. The performance results were a little disappointing, considering it had the newest signature file of the products tested, but our Clean test-set did not trigger any false positives either.

One hundred percent In the Wild detection is expected these days, and *InocuLAN's* ItW Overall score was marred by missing only one sample – one of the No_Frills.Dudley replicants. A very good performance on the Standard test-set was offset somewhat by lower than desirable scores on the Macro and Polymorphic test-sets.

InocuLAN's resident scanner was clearly in the respectable half of the performance overhead distribution, recording the smallest overhead of all products on the 'only monitor file writes' condition. A nice touch with *InocuLAN* is the search option for the on-screen log file.

Command F-PROT v3.0ß 24 March 1997

ItW Boot	100.0%	Macro	96.8%
ItW File	98.1%	Polymorphic	48.4%
ItW Overall	98.8%	Standard	91.0%

Command F-PROT Professional turned in a typically good performance against the In the Wild Boot and File test-sets, missing the single sample of each of the *Word 8* macro viruses and all three samples of Plagiarist.2051 in the ItW File set. With perfect detection of all *Word 6/7* macro viruses, overall detection against the Macro test-set was lowered by failure to detect any *Word 8* or any *Excel* viruses except the Laroux.A samples.

It was somewhat surprising that *Command F-PROT* scored slightly lower than in previous reviews with the same Polymorphic test-set (see the DOS comparative in *VB*, July 1997, p.8). The polymorphics have long been the weak-spot of products based on the *F-PROT* engine, but maybe a more current signature file would have helped too?

Command's on-access component is known as Dynamic Virus Protection (DVP). DVP is either on or off – when on, it monitors file open, close, and rename requests. With greater than a 130% overhead, you will certainly notice DVP's presence working intensively with 'scannable' files.

Cybec VET v9.42 12 June 1997

ItW Boot	100.0%	Macro	97.9%
ItW File	99.4%	Polymorphic	95.1%
ItW Overall	99.6%	Standard	97.4%

A good rule-of-thumb for selecting a scanner based simply on detection is '95% or better on all test-sets'. Although it may have fewer 'perfect 100s' than others, *VET* meets the 95% criterion. The *Word 8* sample of Wazzu.C denied *VET* 100% on the ItW File tests. That virus and all *Excel* viruses

except Laroux.A were all it missed from the Macro test-set. With a very respectable 97.4% detection of the Standard test-set, the Cryptor.2582 stem and eighteen samples of Mad.3544 were responsible for its 95.1% rate against the Polymorphic set. *VET* had no false positives.

VET's resident scanner requires a *Windows* restart for configuration changes to take effect. With the variability in baseline performance from reboot to reboot, these results may be a little less accurate than for the other scanners, whose settings could be changed while they were running. That said, the overhead introduced by *VET's* on-access scanner was the lowest overall, but on the 'write only' condition, *Cheyenne InocuLAN* shone. *VET* was third-fastest on the hard drive tests, with better than twice the throughput of the scanners in the slower half of the test.

Data Fellows F-PROT v2.27 June 1997

ItW Boot	80.2%	Macro	96.8%
ItW File	98.7%	Polymorphic	50.3%
ItW Overall	91.9%	Standard	91.6%

Data Fellows F-PROT Professional was the first of several products in this round-up that suffered from the 'BPB problem' described in our previous *NT* comparative. This causes some detection problems with our In the Wild Boot test-set because some of the infected diskettes have invalid BIOS Parameter Blocks (BPBs).

That *Command's* version successfully detected the viruses on the same diskettes, suggests this is a problem not with the *F-PROT* detection engine, but with the program-to-operating-system interface. (Despite sporting a v3.0 designation, *Command's* product still has the v2.27 engine, so comparisons with that version are relevant.) As these diskettes are infective, this really should be fixed.

Apart from the In the Wild Boot problems, performance of *Data Fellows F-PROT* was similar to *Command's* version. Although detecting nine fewer polymorphics, the higher overall score on that test-set reflects our weighting of reliable detection of polymorphs. The slightly better results in other areas were most likely due to *Data Fellows* having shipped a more current signature file.

Gatekeeper is the on-access component of *Data Fellows F-PROT*, and its configuration options range from active to inactive. With an overhead of 100%, Gatekeeper will make its presence felt.

Dr Solomon's AVTK v7.73

ItW Boot	98.9%	Macro	100.0%
ItW File	100.0%	Polymorphic	97.7%
ItW Overall	99.6%	Standard	100.0%

Excellent all-round performance from the *Anti-Virus Toolkit*, on a par with what has been seen in recent years. A miss on the Moloch boot sector infector was all that kept it from a perfect overall score on the In the Wild tests. 100% on the Macro and Standard test-sets is in line with recent *VB* tests of this product on other platforms.

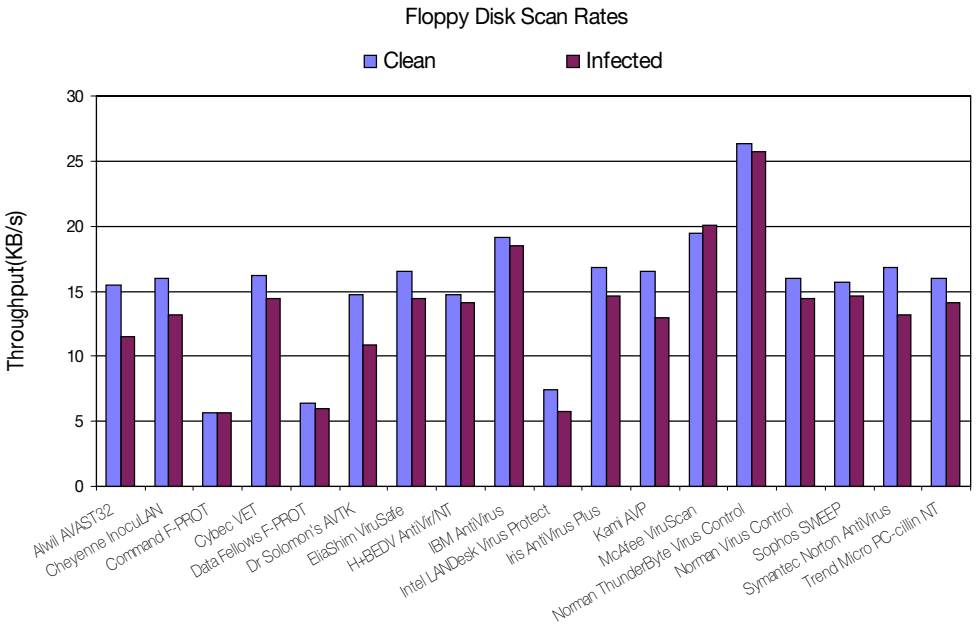
The *AVTK*'s Polymorphic result was down a little from our recent DOS and *Windows 95* comparatives. In those tests the Moloch boot infector and some of the polymorphic samples used in this test were correctly detected.

The *AVTK* is not a speed demon, but scanned our false positive test-set at least twice as quickly as any product in the slowest third of our tests – it also found no 'viruses' there. Coupled with the low overhead of its resident scanner, this is a set of test results to consider seriously.

EliaShim ViruSafe v2.3.9.9

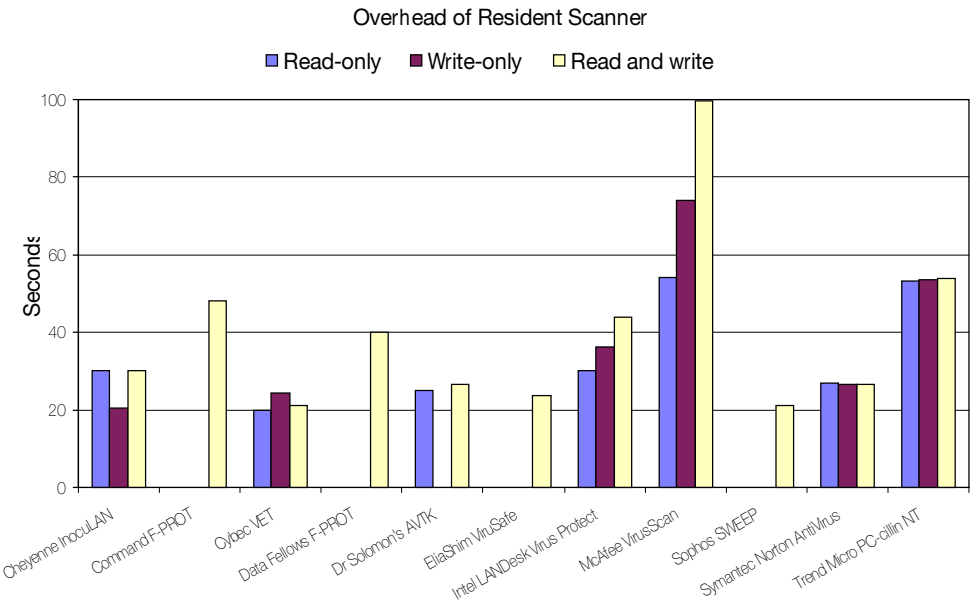
ItW Boot	97.8%	Macro	85.0%
ItW File	99.4%	Polymorphic	83.5%
ItW Overall	98.8%	Standard	97.5%

Missing only Moloch and Hare.7750 in the ItW Boot set and all six Scitzo.1329 replicants in the ItW File set left *ViruSafe* with a very good ItW Overall score. 97.5% on the Standard test-set is also a very good performance, but *ViruSafe* is a little behind the play in the Macro and Polymorphic detection fields. *ViruSafe* did not detect all Laroux.A replicants in the Macro test-set, and had trouble



with some *Word* viruses in files with DOT extensions that it correctly detects in DOC files. The Polymorphic score was seriously degraded by missing just one or two samples of each of several viruses in the test-set.

ViruSafe had the fourth fastest performance on the Clean file set, but still had time to find nine non-existent viruses among the 5500 test files. The resident scanner is either off or scans on all file accesses. It introduced the third smallest overhead for that on-access configuration.



H+BEDV AntiVir/NT v1.01.01

ItW Boot	71.4%	Macro	90.4%
ItW File	91.3%	Polymorphic	72.7%
ItW Overall	83.9%	Standard	90.1%

The *Windows* versions of this German product are still struggling to catch up with the performance of the DOS scanner from *H+BEDV*. Although we ran the tests as Administrator, *AntiVir/NT* could not delete samples that had the read-only file attribute set. Clearing this allowed the tests to run in the desired fashion.

There is no on-access scanner component, and speed against the Clean test-set was in the bottom third of the products tested. *AntiVir/NT* also claimed to detect viruses in the Clean set – seven of them. Some of the configuration screens are still in German, as are the ancilliary utilities such as the scheduler.

IBM AntiVirus v2.52j

ItW Boot	100.0%	Macro	98.9%
ItW File	98.7%	Polymorphic	96.2%
ItW Overall	99.2%	Standard	99.7%

The two *Word 8* Wazzu variants denied *IBM AntiVirus* 100% detection on the ItW File (and consequently ItW Overall) and the Macro test-sets. An excellent all-round performance.

Although several products offer file checksumming as an option to improve speed and to provide a degree of detection for unknown viruses, *IBM AntiVirus* has this feature as an integral part of the scanner. For this reason we ran the speed tests twice for this product. The reported results are from the second run, indicating the typical usage of the scanner. Placing second fastest with this result, you should note that updates to the products will cause a recalibration of the checksum database and the first scan following an update will take approximately four times as long (still faster than the five slowest scanners in our test!).

Intel LANDesk Virus Protect v5.0RC

ItW Boot	90.1%	Macro	80.7%
ItW File	98.3%	Polymorphic	85.9%
ItW Overall	95.3%	Standard	97.2%

Intel supplied Release Candidate code for this review, and v5.0 is now shipping. *LANDesk Virus Protect* has not been renowned for its detection rates, but it has been gradually improving in this respect over the last year or so. This review sees a noticeable increase in its detection of the Standard test-set and a very respectable 98.3% against the ItW File set. However, seeing any scanner miss ten-year old boot viruses like Stoned.Standard is a little sad…

Against the clock, *LANDesk Virus Protect* was in the bottom five – maybe reporting five viruses in the Clean set slowed it down? Its on-access scanner overhead was middle of the pack.

Iris AntiVirus Plus v22.0 30 June 1997

ItW Boot	100.0%	Macro	94.3%
ItW File	99.7%	Polymorphic	87.4%
ItW Overall	99.8%	Standard	98.9%

One of the two No_Frills_Dudley samples accounted for *Iris AntiVirus Plus* missing a perfect score on the In the Wild File set and In the Wild Overall. With a good performance on the Macro test-set, and a very creditable 98.9% on the Standard test-set, work on detection of some of the more complex polymorphics would boost *AntiVirus Plus* into the top group.

Unfortunately, these good detection rates were offset by very slow scanning speeds. *AntiVirus Plus* also took the wooden spoon for most false positives in this review – at 139 of them, this was more than four times as many as all the other products combined! There is no resident scanner.

KAMI AVP v3.0 19 June 1997

ItW Boot	82.4%	Macro	100.0%
ItW File	99.7%	Polymorphic	95.2%
ItW Overall	93.3%	Standard	98.8%

One of the two Avispa.D samples prevented *AVP* registering a perfect score on the ItW File set. A serious case of the BPB problem saw an uncharacteristically low ItW Boot score for *KAMI's* product. 100% detection on the Macro test-set is an excellent result by any standard, and 98.8% on the Standard set is also a very good result.

AVP placed mid-way on scanning speed and flagged six files as 'suspicious' and claimed two working executables were 'corrupted'. Although not true false positives, such reports can generate many time-wasting support calls in a large organization. *AVP* has no on-access scanner.

McAfee VirusScan v3.0.2/3006

ItW Boot	100.0%	Macro	100.0%
ItW File	100.0%	Polymorphic	98.7%
ItW Overall	100.0%	Standard	98.4%

'Big' is a word associated with *McAfee* – it applies equally well to its industry presence, product popularity, and lawsuits. It also applies to *VirusScan's* detection scores. With 100% on the ItW and Macro test-sets and only missing a small handful of samples on the Polymorphic and Standard test-sets, *VirusScan* was one of the top scorers, overall.

'Big' also applies to *VirusScan's* times on the Clean test-set, where it was second slowest; just faster than *AVAST32*. To really confuse things, *VirusScan* was second fastest on the floppy disk scanning speed test.

VirusScan's on-access scanner had far and away the highest performance overhead of the products tested. In fact, the smallest on-access overhead recorded with *McAfee's* product was greater than the largest overhead of any configuration of any other product's resident scanner. The developers should look into this, as operations that take twenty seconds normally can take nearly 100 seconds with their on-access scanner active.

Norman ThunderByte Virus Control v8.01

ItW Boot	82.4%	Macro	100.0%
ItW File	100.0%	Polymorphic	93.5%
ItW Overall	93.5%	Standard	97.8%

Norman's assimilation of the *ESaSS* product range is starting to show in a name change for the venerable *ThunderByte*. Despite 100% against the ItW File set, *NTVC* fell foul of the BPB problem, resulting in a badly depressed ItW Boot and ItW Overall score. Same comment as elsewhere – these diskettes are infective so they should be detected. A perfect score on the Macro test-set and a very good performance against the Standard set were offset by a slightly lower, but still respectable, score against the Polymorphic test-set.

The name change certainly hasn't affected the scanning speed, again being the faster performer against the Clean test-set, but it did raise one false-positive. *NTVC* does not have an on-access scanner.

Norman Virus Control v4.2

ItW Boot	100.0%	Macro	99.6%
ItW File	100.0%	Polymorphic	88.5%
ItW Overall	100.0%	Standard	92.2%

Norman Virus Control's results are in line with its recent form on *VB* comparatives. Perfect scores on the ItW sets and near-perfect detection of the Macro test-set, but with noticeably lower performance on the 'zoo' viruses, reflect the priorities of most anti-virus companies these days.

Scanning speed against the Clean set was solidly middle of the range and *NVC* correctly failed to find any viruses in this test. A resident scanning module was shipped with the product, but this kept dying part-way through the copying process in our overhead tests. *Norman* confirmed such a problem with this release of *NVC* 'on some machines' and expected to ship a fix with the next version.

Sophos SWEEP v2.99 1 July 1997

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

SWEEP had excellent detection in all test-sets, with two samples of Positron from the Standard test-set its only misses across all of the tests. *SWEEP* is not the fastest scanner, but is in the top half of the draw in this regard. No false positives were reported.

InterCheck, *SWEEP's* resident scanner, has various configuration options concerning which files to scan and what scan modes to use, but as with several other products it is either on or off. This should not be a serious concern however, as it offered the second-lowest overhead in the 'all access' condition, just 0.1% greater than *Cybec's VET*.

InterCheck's low overhead on this test is due to its use of a checksumming technique, allowing it to decide quickly whether files it has seen before have changed and if not, it does not scan them again. In these tests we allowed

InterCheck to build its checksum database, disabled on-access scanning, ran the baseline test then re-enabled on-access scanning and ran the overhead test. The measured overhead will be lower than on newly-created or modified files. Also, each upgrade of the software will see a larger, one-off overhead as each existing file is accessed, as these have to be checked for viruses added to the product since the last upgrade.

Symantec Norton AntiVirus v2.01 1 July 1997

ItW Boot	100.0%	Macro	97.9%
ItW File	99.7%	Polymorphic	87.5%
ItW Overall	99.8%	Standard	96.9%

Symantec's NAV turned in very good performances, consistent with its stablemates' in our recent comparatives. One of the Desperado.1403 samples was the only miss in the ItW File test-set. The Polymorphic test-set is still *NAV's* Achilles heel – apart from there, *NAV* surpassed the 95% mark on all tests.

Scanning speed was quite acceptable – in the top third but noticeably slower than the top three. *NAV's* on-access scanner overhead was around 33% regardless of configuration options. That may seem high, but is in the better half of the test results, and allowing for the nature of the overhead test, is probably quite acceptable in everyday use.

Trend Micro PC-cillin NT v1.0 3 July 1997

ItW Boot	95.6%	Macro	97.3%
ItW File	99.0%	Polymorphic	89.7%
ItW Overall	97.7%	Standard	94.7%

Hovering around 98%, the ItW overall score for *Trend's PC-cillin NT* performance was similar to that of its siblings in recent *VB* comparative tests. However, its Macro and Standard detection rates have improved noticeably since the July DOS comparative.

The scanner was among the slowest tested. This is also reflected in its resident scanner overhead being higher than all other products except *McAfee's VirusScan*. As with *H+BEDV's AntiVir/NT*, the read-only attribute was enough to stop *PC-cillin NT* from deleting infected files, even though it was running as Administrator.

Conclusion

In alphabetical order, *Cybec's VET*, *Dr Solomon's AVTK*, *IBM AntiVirus*, *McAfee VirusScan*, and *Sophos' SWEEP* are the best performers in terms of virus detection. There are large differences in speed and on-access overhead. With the increasing importance of the latter in catching Internet download and email-borne viruses, this will likely inform many buying choices. Overall, it is good to see the level of detection improving slightly (BPB problems aside!).

Technical Details

Test environment: *Compaq* Prolinea 590, 80 MB RAM, 2.1 GB hard disk and 270 MB *SyQuest* removable cartridge drive, running *Microsoft Windows NT Workstation v4.0* with Service Pack 1.

Speed test-sets: Clean floppy: 43 COM/EXE files, occupying 997,023 bytes on a 1.44 MB diskette. Infected floppy: The same files infected with Natas.4744, occupying 1,201,015 bytes on a 1.44 MB diskette. Clean Hard Disk: 5500 COM/EXE files, occupying 546,932,175 bytes, copied from CD-ROM to hard disk.

VIRUS TEST-SETS

In the Wild Boot Sector test-set. 91 samples of 91 viruses, one each of:

15_Years, AntiCMOS.A, AntiCMOS.B, AntiEXE.A, Boot437, Bootexe.451, Brasil, Bye, Chance.B, Chinese_Fish, Crazy_Boot, Cruel, Da'Boys, Defo, DelCMOS.B, Den_Zuko.2.A, Diablo_Boot, Disk-Killer.1_00, Empire.Int_10B, Empire.Monkey.A, Empire.Monkey.B, Exe_Bug.A, Exe_Bug.C, Exe_Bug.Hooker, FAT_Avenger, FinnishSprayer, Flame, Form.A, Form.C, Form.D, Frankenstein, Galicia, Hare.7750, Ibex, Int40, J&M, Joshi.A, Jumper.A, Jumper.B, Junkie.1027, Kampana.A, Leandro, Michelangelo.A, Misis, Moloch, Mongolian_Boot, Music_Bug, Natas.4744, Neuroquila.A, NYB, Ornate, Parity_Boot.A, Parity_Boot.B, Pasta, Paula_Boot, Peter, Qrry, Quandary, Quiver, Quox.A, Ripper, RP, Russian_Flag, Sampo, Satria.A, She_Has, Stealth-Boot.B, Stealth-Boot.C, Stoned-W-Boot, Stoned.16.A, Stoned.Angelina.A, Stoned.Asuza.A, Stoned.Bravo, Stoned.Bunny.A, Stoned.Daniella, Stoned.Dinamo, Stoned.June-4th.A, Stoned.Kiev, Stoned.LZR, Stoned.Manitoba, Stoned.NO_INT_A, Stoned.NOP, Stoned.Spirit, Stoned.Standard.A, Stoned.Swedish-Disaster, Swiss_Boot, Unashamed, Urkel, V-Sign, WelcomB, and WXYC.

Polymorphic test-set. 13,000 samples of 26 viruses, 500 each of:

Alive.4000, Anarchy.6503, Arianna.3076, Baran.4968, Code.3952:VICE.05, Cordobes.3334, Cryptor.2582, Digi.3547, DSCE.Demo, Girafe:TPE, Gripe.1985, Groove_and_Coffeeshop, Mad.3544, MTZ.4510, Natas.4744, Neuroquila.A, Nightfall.4559.B, One_Half.3544, Pathogen:SMEG.0_1, PeaceKeeper.B, Russel.3072.A, SatanBug.5000.A, Sepultura:MtE-Small, SMEG_v0.3, Tequila.A, and Uruguay.

Macro test-set. 722 samples of 182 viruses, made up of:

ABC.A (4), Alien.A (4), Alien.B (4), Alliance.A (4), AntiConcept.A (4), Appder.A (4), Appder.B (4), Atom.A (4), Atom.B (4), Atom.C (4), Atom.D (4), Atom.E (4), Atom.G:De (4), Atom.H (4), Baby.A, BadBoy.A, BadBoy.B (4), Bandung.A (4), Bandung.G (4), Bandung.H (4), Bandung.I (4), Bandung.N (4), Birthday.A:De (4), Boom.A (4), Boom.B (4), Buero.A:De (4), Cap.A (4), CeeFour.A (4), Chaos.A (4), Clock.A:De (4), Clock.B:De (4), Clock.C:De (4), Clock.D:De (4), Clock.E:De (4), Clock.F:De (4), Colors.A (4), Colors.B (4), Colors.C, Colors.D (2), Colors.E (4), Colors.F (4), Colors.H (4), Colors.J (4), Colors.K (4), Colors.M (4), Colors.P (4), Concept.A (4), Concept.AA (4), Concept.B:Fr (4), Concept.C (4), Concept.D (4), Concept.E (4), Concept.F (4), Concept.G (4), Concept.H (4), Concept.J (4), Concept.L (4), Concept.M (4), Concept.W (4), Concept.X (4), Concept.Y (4), Concept.Z (4), CountTen.A (4), Daniel.A (4), Daniel.B (4), Daniel.C (4), Dark.A (4), Date.A (4), Delta.A (3), Dietzel, Divina.A, Divina.C (4), Divina.E, DMV.A (4), DMV.B (4), DMV.C (4), Doggie.A (4), DZT.A (4), Easy.A (4), Friday.A:De (4), Gable.A (4), Gangsterz.A (4), Goldfish.A (4), Hassle.A (4), Hellgate.A (4), Helper.A (4), Hot.A (4), Hybrid.A (4), Hybrid.B (4), Imposter.A (4), Irish.A (4), Irish.B (4), Irish.C (4), Johnny.A1 (4), Johnny.B (4), KillDLL.A (4), Kompu.A (4), Laroux.A (4), Legend.A (4), Lunch.A (4), Lunch.B (4), MadDog.A (4), MadDog.B (4), MDMA.A (4), MDMA.C (4), MDMA.D (4), MDMA.E (4), MDMA.F (4), Minimal.A (4), Minimal.B (4), Minimal.D (4), Muck.A, NF.A (4), NiceDay.A (4),

NiceDay.B (4), Nightshade.A (4), Nomvir.A:De (4), Nop.A:De (4), Nop.B:De (4), Nop.D:De (4), NPad.A (4), NPad.K (4), NPad.Q (4), NPad.S (4), Nuclear.A (4), Nuclear.B (4), Nuclear.E (4), Outlaw.A (4), Paper.A (4), Paycheck.A (4), Phadera.A (4), Phadera.B (4), Polite.A (4), Rapi.A (4), Rapi.A2 (4), Rapi.B, Rapi.G, Rapi.H2 (4), Rats.A (4), Rats.B (4), Rats.C (4), Robocop.A (4), Satanic.A (4), Saver.A (4), Sharefun.A (4), ShowOff.A (4), ShowOff.B (4), ShowOff.C (4), ShowOff.G (4), Smiley.A (4), Smiley.B:De (4), Spiral.A (4), Spooky.A:De (4), Stryx.A (4), SwLabs.A (4), Tedious.A (4), Tele.A:De (4), Twister.A (4), TwoLines.A (4), Wazzu.A (4), Wazzu.AF (4), Wazzu.AH (4), Wazzu.AJ (4), Wazzu.AK (4), Wazzu.AL (4), Wazzu.AM (4), Wazzu.AN (4), Wazzu.AO (4), Wazzu.AR (4), Wazzu.AS (4), Wazzu.AU (4), Wazzu.B (4), Wazzu.C (4), Wazzu.E (4), Wazzu.F (4), Wazzu.H (4), Wazzu.J (4), Wazzu.L (4), Wazzu.O (4), Wazzu.P (4), Wazzu.X (4), Wazzu.Y (4), and Wazzu.Z (4).

In The Wild File test-set. 530 samples of 147 viruses, made up of:

Alfons.1344 (5), Anticad.4096.Mozart (4), Arianna.3375 (4), Avispa.D (2), Backformat.2000.A, Bad_Sectors.3428 (5), Barrotes.1303 (6), Barrotes.1310.A (2), BootEXE.451 (3), Burglar.1150.A (3), Byway.A, Byway.B, Cascade.1701.A (3), Cascade.1704.A (3), Cawber (3), Changsa.A (5), Chaos.1241 (6), Chill, Cordobes.3334 (3), CPW.1527 (4), Dark_Avenger.1800.A (3), Delta.1163 (6), DelWin.1759 (3), Desperado.1403.C (2), Die_Hard (2), Digi.3547 (5), Dir_II.A, Ear.Leonard.1207 (3), Fairz (6), Fichv.2_1 (3), Flip.2153.A (2), Flip.2343 (6), Freddy_Krueger (3), Frodo.A (4), Ginger.2774 (2), Goldbug (3), Green_Caterpillar.1575 (3), Hare.7610 (2), Hare.7750 (8), Hare.7786 (9), Helloween.1376.A (6), Hi.460 (3), Hidenowt (6), HLLC.Even_Beeper.B (3), Istanbul.1349 (6), Jerusalem.1244 (6), Jerusalem.1500 (3), Jerusalem.1808.Standard (2), Jerusalem.Mummy.1364.A (3), Jerusalem.Sunday.A (2), Jerusalem.Zero_Time.Australian.A (3), Jos.1000 (3), Junkie.1027, Kaos4.697 (6), Karnivali.1971 (3), Keypress.1232.A (2), Lemming.2160 (5), Liberty.2857.A (2), Little_Red.1465 (2), MacGyver.2803 (3), Major.1644 (3), Maltese_Amoeba (3), Mange_Tout.1099 (4), Manzon.1414 (2), Markt.1533 (3), Mirea.1788 (2), Natas.4744 (5), Necros.1164 (2), Nightfall.4518.B (2), No_Frills.Dudley (2), No_Frills.No_Frills.843 (2), Nomenklatura.A (6), November_17th.800.A (2), November_17th.855.A (2), NPox.963.A (2), One_Half.3544 (5), One_Half.3570 (3), Ontario.1024 (3), Pathogen:SMEG.0_1 (5), Ph33R.1332 (5), Phx.965 (3), Pieck.4444 (3), Plagiarist.2051 (3), Predator.2448 (2), Prudents.1205.A, Quicky.1376, Reverse.948 (3), Sarampo.1371 (6), Sat_Bug (2), Sayha (5), Scitzo.1329 (6), Screaming_Fist.II.696 (6), Sibylle (3), Sleep_Walker.1266 (3), SVC.3103.A (2), Tai-Pan.438 (3), Tai-Pan.666 (2), Tanpro.524 (6), Tentacle.10634 (4), Tentacle.1996 (3), Tequila.A (3), Three_Tunes.1784 (6), Trakia.653 (3), Tremor.4000.A (6), Trojector.1463 (6), Trojector.1561 (3), TVPO.3873 (9), Unsnared.814 (3), Vacsina.TP-05.A (2), Vacsina.TP-16.A, Vampiro (2), Vienna.648.Reboot.A (3), Vinchuca (3), VLamix (3), Werewolf.1500.B (3), Xeram.1664 (4), Xuxa.1984 (6), Yankee_Doodle.TP-39 (5), Yankee_Doodle.TP-44.A (5), and Yankee_Doodle.XPEH.4928 (2).

…along with the following macro viruses:

Appder.A (4), Bandung.A (4), Boom.A:De (4), Buero.A:De (4), CAP.A (4), Colors.A (4), Concept.A (4), Concept.F (4), Concept.J (4), Date.A (4), Divina.A (4), Helper.A (4), Hot.A (4), Hybrid.A (4), Imposter.A (4), Irish.A (4), Johnny.A (4), Laroux.A (4), MDMA.A (4), MDMA.D (4), NiceDay.A (4), NJ-WMDLK1.A (4), NK-WMDLK1.B (4), NOP.A:De (4), NPad.A (4), NPad.D (4), Nuclear.B (4), Rapi.A (4), Sharefun.A (4), Wazzu.A (4), Wazzu.C (4), Wazzu.E (4), Wazzu.F (4), Wazzu.J (4), Wazzu.P (4), Wazzu.X, W97M/Wazzu.A, and W97M/Wazzu.C.

Standard test-set. 774 samples of 321 viruses, made up of:

Abbas.5660 (5), Accept.3773 (5), Account_Avenger.873 (3), Aforia.656 (6), AIDS, AIDS-II, Aiwed.852 (3), Alabama, Alexe.1287 (2), Algerian.1400 (3), Amazon.500 (2), Ambulance, Amoeba (2), Anarchy.6503 (5), Andreew.932 (3), Angels.1571 (3), Annihilator.673 (2), Another_ World.707 (3), Anston.1960 (5), Anthrax, Anti-Pascal (5), Anticad.4096.A (4), AntiGus.1570 (3), Argyle, Armagedon.1079.A, Assassin.4834 (3), Assignation.426 (3), Attention.A, Auspar.990 (3), Autumnal.3072 (6), Baba.276 (3), Baba.356 (2), Backfont.905, Barrotes.840 (3), Beast.498 (2), Bebe.1004, Bell.390 (3), Big_Bang.346, Bill.2658 (5), Billy.836 (3), Black_Monday.1055 (2), BlackAdder.1015 (6), Blood, Blue_Nine.925.A (3), Bosnia:TPE.1_4 (5), Burger (3), Burger.405.A, Burglar.824 (3), Butterfly.302.A, BW.Mayberry.499 (3), BW.Mayberry.604 (6), Cantando.857 (3), Cascade.1701.Jo-Jo.A, Cascade.1704.D (3), Casper, Catherine.1365 (3), CeCe.1998 (6), CLI&HLT.1345 (6), Cliff.1313 (3), CMOS.3622 (5), Coffeeshop (2), Continua.502.B (3), Cool.929 (3), Cosenza.3205 (2), Cowboy.2487 (2), Coyote.1103 (3), Crazy_Frog.1477 (3), Crazy_Lord.437 (2), Cruncher (2), Cybercide.2299 (3), Danish_Tiny.163.A, Danish_Tiny.333.A, Dark_Avenger.1449 (2), Dark_Avenger.2100.A (2), Dark_ Revenge.1024 (3), Darkstar.439, Datacrime (2), Datacrime_II (2), Datalock.920.A (3), DBF.1046 (2), Dei.1780 (4), Despair.633 (3), Destructor.A, Diamond.1024.B, Dir.691, Discoloured_Star.223, DOSHunter.483, DotEater.A, DR&ET.1710 (3), Ear.405 (3), Eddie-2.651.A (3), Eight_ Tunes.1971.A, Emhaka.749 (6), Enola_Gay.1883 (4), Entity.1980 (5), F-You.417.A, Fax_Free.1536.Topo.A, Fellowship, Feltan.565 (3), Finnish.357 (2), Fisher.1100, Flash.688.A, Four_Seasons.1534 (3), Frodo.3584.A (2), Fumble.867.A, Genesis.226, Glacier.1196 (2), Golden_ Flowers.1688 (6), Gomer.691 (6), Gotcha.906 (6), Green.1036 (6), Greetings.297 (2), Greets.3000 (3), Halka.1000.b (3), Halloechen.2011.A (3), Hamme.1203 (6), Happy_New_Year.1600.A, Hasta.884 (2), HDZZ.566 (3), Helga.666 (2), Helga.666.c (2), Hideos.1028 (6), HLLC.Even_Beeper.A, HLLC.Halley, HLLP.5000 (5), HLLP.7000 (5), HN.1741 (3), Horsa.1185 (3), Hymn.1865.A (2), Hymn.1962.A (2), Hymn.2144 (2), Hypervisor.3128 (5), Ibqqz.562 (3), Icelandic.848.A, Immortal.2185 (2), Inferno.1800 (4), Internal.1381, Intruder.2048 (3), Invisible.2926 (2), Itavir.3443, IVP.1725 (3), Jerusalem.1607 (3), Jerusalem.1808.CT.A (4), Jerusalem.Fu_Manchu.B (2), Jerusalem.PcVrsDs (4), John.1962 (3), Joker, Joker.1570 (6), July_13th.1201, June_12th.2660 (6), June8th.1919 (6), June_16th.879, Kamikaze, Kela.B.2018 (3), Kemerovo.257.A, Keypress.1280 (6), Khizhnjak.556 (3), Kode.145 (3), Korea_Eddy.1316 (6), Korea_Miny.218 (3), Korea_Wanderer.1756 (6), Kranz.255 (3), Kukac.488, Lauren.632 (3), Lavi.1460 (3), Leapfrog.A, Leda.820 (3), Lehigh.555.A, Liata.327 (3), Liberty.2857.A (5), Liberty.2857.D (2), Liquid_Power.1016 (3), Little_ Brother.307, Loren.1387 (2), Lost_Love.853 (6), LoveChild.488, Lutil.591 (3), Maresme.1062 (3), MemLapse.289 (3), Metabolis.1173 (3), Mickie.1100 (3), Midin.765 (2), MonAmi.1085 (3), Monster.424 (3), Mothership.655 (3), MPC.442.c (3), Mummy.1353 (3), Necropolis.1963.A, Nina.A, November_17th.768.A (2), NRLG.1038 (3), NutCracker.3500.D (5), Odious.569 (3), Omud.512, On_64, Oropax.A, Pamyat.2000 (2), Parity.A, Paulus.1804 (5), Peanut, Perfume.765.A, Phantom1 (2), Phoenix.800, Pitch.593, Piter.A (2), Pixel.847.Hello (2), Pizelun (4), Plague.2647 (2), Poison.2436, Pojer.4028 (2), Positron (2), Power_Pump.1, PS-MPC.227 (3), PS-MPC.545 (6), QPA.256 (3), Quark.A, Red_Diavolyata.830.A, Revenge.1127, Riihi.132, Rmc.1551 (4), Rogue.1208 (6), Rosebud.912 (3), Rubbit.734 (2), Saturday_14th.669.A, Screaming_Fist.927 (4), Screen+1.948.A, Selfex.1472 (6), Semtex.1000.B, Senorita.885 (3), Shake.476.A, ShineAway.620 (3), SI.A, SillyC.226 (3), SillyCR.303 (3), SillyCR.710 (3), Sofia.43 (3), Soup.1073 (3), Spanz.639 (2), Stardot.789.A (6), Stardot.789.D (2), Steatoda (6), Stud.347 (3), Subliminal, Suomi.1008.A, Suriv_1.April_1st.A, Suriv_2.B, Surprise.1318, SVC.1689.A (2), Svin.252 (3), Svir.512, Sylvia.1332.A, SysLock.3551.H (2), TenBytes.1451.A, Teraz.2717 (5), Terror.1085, Thanksgiving.1253, The_Rat, Tigre.1795 (6), Tiny.133, Tiny.134, Tiny.138, Tiny.143, Tiny.154, Tiny.156, Tiny.158, Tiny.159, Tiny.160, Tiny.167, Tiny.198, Todor.1993 (2), Traceback.3066.A (2), Trivial.113 (3), TUQ.453, Untimely.666 (3), V2P6, V2Px.1260, Vacsina.1212, Vacsina.1269, Vacsina.1753, Vacsina.1760, Vacsina.1805, Vacsina.2568, Vacsina.634 (1), Vacsina.700 (2), Vbasic.5120.A, VCC.350 (3), Vcomm.637.A (2), VCS1077.M, VFSI, Victor, Vienna.583.A, Vienna.623.A, Vienna.648.Lisbon.A, Vienna.Bua (3), Vienna.Monxla.A, Vienna.W-13.507.B, Vienna.W-13.534.A, Vienna.W-13.600 (3), Virogen.Pinworm (6), Virus-101, Virus-90, Voronezh.1600.A (2), Voronezh.600.A, VP, Warchild.886 (3), Warrior.1024, Whale, Willow.1870, WinVir, WW.217.A, XWG.1333 (3), Yankee_Doodle.1049 (1), Yankee_Doodle.2756, Yankee_Doodle.2901, Yankee_Doodle.2932, Yankee_Doodle.2981, Yankee_Doodle.2997, Zany.225 (3), Zero_Bug.1536.A, and Zherkov.1023.A.

VIRUS BULLETIN **©1997 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /97/$0.00+2.50**

PRODUCT REVIEW 1

Dr Solomon's AVTK v7.72 for NetWare

Martyn Perry

The standard server licence for this product covers one server per workstation, with additional workstations licensed separately. All diskettes supplied have individual serial numbers. The copy sent for review was a packaged set comprising nine, 3.5-inch floppy disks: four for DOS, one for *Windows*, three for *NetWare* and the Magic Bullet. The latter is a boot disk with the FV86.exe scanner which takes a two-pass approach**.** Some indication of program activity during its first pass would be helpful.

The product's comprehensive documentation consists of 'Anti-Virus Toolkit for NetWare', 'Anti-Virus Toolkit for DOS & Windows', 'Virus Encyclopædia', 'Windows 3.x Installation Card', and lastly 'Installation Changes for Version 7.72'. Primarily, these changes will affect users who upgrade their scanners with a customized process, which is important because there will be new and additional files to be added to any script and some existing files will have been rendered obsolete.

Installation

The *AVTK v7.72* requires CLIB version 3.12g or later, for *NetWare 3.x*, and AFTER311.NLM and NWSNUT.NLM for all versions of *NetWare*. The installation guide advises attaching to the target server as supervisor, thus preventing a login script from calling possibly infected executables. Running the installation program from a workstation, existing files are updated and new files copied to the appropriate directories. The Configuration Editor files can be copied to the system administrator's workstation if desired, and desktop icons or short-cuts to them created.

Once installed, the *AVTK for NetWare* is loaded from the server console like any other NLM. Once loaded, the *AVTK* scheduler can be stopped by pressing the Esc key.

Configuration Options

The scheduler is very much at the heart of the *NetWare* scanner. It has four monitors, with four different functions, each covering separate aspects of server protection. A connection monitor tracks workstations as they log in to the server to ensure that they are running VirusGuard, the on-access component of *Dr Solomon's* workstation anti-virus software. Another monitor tracks volumes as they are mounted, running *NetWare* FindVirus on any new one. On-access scanning is controlled by a third monitor (more of this later), while the fourth detects any virus alerts and handles the responses.

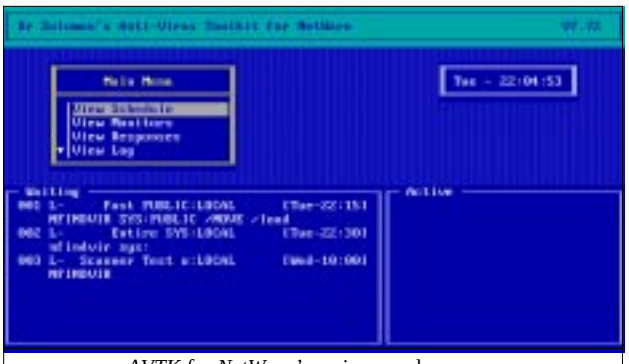
The scheduler itself is controlled by an ASCII configuration file (the default is NTOOLKIT.CFG). It is possible to prepare several configuration files and specify which to load when starting the scheduler. The configuration file can be edited with any ASCII editor, but it is more convenient to make use of the *Windows*-based Configuration Editor (NTKEDIT) supplied with the *ATVK*.

The menu options, along with the activity screen, are shown on the scheduler's main screen, which is split into two display panels. The 'Waiting' panel lists scheduled events awaiting a trigger, while 'Active' displays any currently active scheduled events.

Three modes of operation are available. A scheduled scan can be started immediately by pressing F6 on the server console. Unfortunately, *Dr Solomon's* still chooses to keep the stop command undocumented. Alternatively, the File Access Monitor (FAM) allows scanning to be performed when a file is read or written, when a volume is mounted, or when a user attempts to log on. The third option is a scheduled function which uses the settings defined in the CFG file. Time schedules for a scan can be set to yearly, monthly, weekly, daily, hourly or custom. Custom allows the scan to be repeated every *n* minutes.

The Configuration Editor has an option to make the FAM reread any changes made to the configuration file while the FAM is running. This is in contrast to the scheduler itself, which must be unloaded and reloaded before any configuration changes take effect. The Configuration Editor also defines the options for *NetWare* FindVirus. These include selection of the volumes to scan; extensions of files to check; the choice of repair options; location and name of report files; and some options not available from the menus. These choices build up a command-line which is displayed in the bottom of the window.

In the event of a virus being detected, a range of actions is available. The infection can be merely reported, with no further action taken, or FindVirus can attempt to repair the file. If an infected file cannot be repaired, it is renamed and



AVTK for NetWare's main console screen.

its Inherited Rights Mask is set to prevent access (unless the user has supervisor privileges). Another option is to move all infected files to the Move/Backup directory, before FindVirus goes to work. An original file which cannot be repaired is deleted and purged. Alternatively, all infected files can be moved to the Move/Backup directory. If an attempt to move a file fails, it is renamed and its Inherited Rights Mask set to prevent users without supervisor privileges from accessing it. The default Move/Backup directory is CONFINED.VIR, located in the root directory of the scanned volume. If a file is moved to it, the original path as well as filename is stored here. This can help in identifying the possible source of infection.

All output is written to the console screen with the option to write reports to a text file. Unless otherwise specified, the default name is REPORT.TXT. A separate *NetWare* print queue can be specified for the report output.

Alert Management

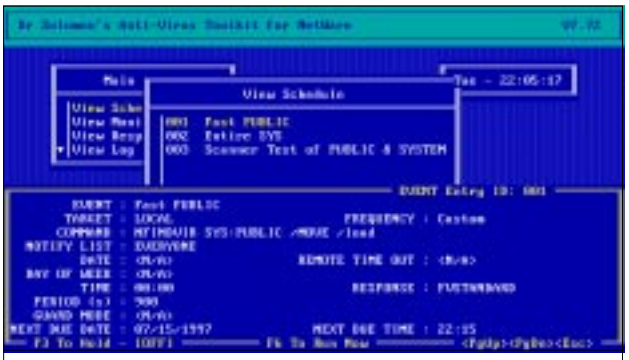
AVTKN operates alert management by making use of response tables, lists of codes returned by the scanner in response to different events. They are similar to DOS errorlevels but much more sophisticated.

Any result produced by either a local or remote process is compared to the entries in the tables. The matching entry specifies an appropriate message and a list of actions for that message. These various actions can be selected for the specific code. They include sending the message to either an application log or the server console, broadcasting it to the users on the notification list, or setting the hold flag. The workstation can also be disconnected from the server, or ordered to log out from all servers.

Three such tables are set up by default. The INTERNAL response table deals with standard and internal errors, such as time-outs and communication errors. FVSTANDARD handles standard FindVirus results – no virus found, file access problem and virus found. Finally, the FVEXTENDED table manages the extended results which give details of the nature of the problem.

The scanner NFINDVIR can be loaded directly from the console. Its command-line options are very similar to those of the DOS scanner, but with server-specific variations such as /ALLVOLUMES and support for checking files migrated to/from HSMs. If the supervisor prefers not to define scan options directly, they can use the NFINDVIR.INI file which stores the option settings permanently.

The DOS workstation is protected by VirusGuard, or in the case of *Windows*, WinGuard, both licensed separately. These are used in conjunction with FAM to provide the means for virus infection warnings, which is particularly relevant when a workstation first attempts to log on. Protection is provided in two stages. First, the workstation is checked for VirusGuard, and second, a command is issued – usually, but not always, an order to run FindVirus.



The heart of *AVTKN's* scheduler…

Updates and Results

Updates are supplied as physical media and can be installed using customized scripts or as a standard installation.

The scanner was checked using the four test-sets – In the Wild File, Standard, Macro and Polymorphic (see summary for detail). The virus signature list used a virus driver dated 21 April 1997, detecting 12,117 viruses, Trojans and variants. Undetected viruses were identified by using the move infected files option and listing the files left in the virus directories. The tests were conducted using the default scanner file extensions supplied.

Both the In the Wild File and Macro virus tests resulted in 100% detection. The Standard test failed on two samples of Midin.765, and the Polymorphic test dropped a few brownie points, missing thirteen samples of Baran.4968 and 138 samples of Cryptor.2582.

To determine the impact of the scanner on the active server, the following test was executed. Its basis was to time the copy of 63 files of 4,641,722 bytes (EXE files from SYS:PUBLIC) from one server directory to another using *Novell's* NCOPY. This kept data transfer within the server itself and minimized network effects. The directories used for the source and target were excluded from the virus scan so as to avoid the risk of a file being scanned while waiting to be copied. Due to the different processes which occur within the server, the time tests were run ten times for each setting and an average taken.

The conditions for each of the tests were:

- NLM not loaded. This establishes the baseline time for the copying process.
- NLM loaded, FAM = No, Read Files = No, Write Files = No, Scan = No. This tests the impact of the scanner loaded in its quiescent state with no real-time or immediate scan in progress.
- NLM loaded, FAM = Yes, Read Files = No, Write Files = No, Scan = No**.** This shows the effect of the real-time scan NLM being loaded.
- NLM loaded, FAM = Yes, Read Files = Yes, Write Files = No, and Scan = No. This shows the on-access scan effect when reading files.

- NLM loaded, FAM = Yes, Read Files = No, Write Files = Yes, and Scan = No. This shows the on-access scan effect when writing files.
- NLM loaded, FAM = Yes, Read Files = Yes, Write Files = Yes, and Scan = No. This shows the overhead of having both read and write scans in effect.
- NLM loaded, FAM = Yes, Read Files = Yes, Write Files = Yes, and Scan = Yes. This shows the effect of running an on-demand scan as well as the real-time scan.
- NLM unloaded**.** This is run after the other tests to check how well the server returns to its former state.

The results of these tests are presented in the summary box at the end of this review.

The initial impact of loading the on-access scanner is minimal. However, it begins to take effect when one of the real-time scans is selected. Oddly, the impact of the write overhead is very much lower than when reading the file. Even when the scanner is running, the overall performance hit is much lower than many other products.

Conclusion

Although this product looks very similar to the one reviewed by *VB* in December 1995, the virus world and its underlying support has become more sophisticated. Back then, boot sector viruses predominated and macro viruses had only just been seen out in the wild. How things change!

In fact, *AVTKN's* detection rate still remains one of the best around, despite a minor hiccup in the polymorphics. The on-access overhead is one of the lowest that I have encountered in testing. On the minus side, it is disappointing to see that there is still no real multi-server support. The response tables can be used to trigger actions and send warnings remotely, but this does not provide a convenient method of multi-server management. Apart from this one gripe, it is good to see the product keeping abreast of virus developments and evolving to give the user the same 'industrial strength' protection.

Dr Solomon's AVTK for NetWare v7.72

Detection Results

Test-set[1]	Viruses Detected	Score
In the Wild File	549/549	100.0%
Standard	772/774	99.7%
Polymorphic	12849/13000	98.8%
Macro	716/716	100.0%

Overhead of On-access Scanning:

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

	Time	Overhead
Baseline	6.8	–
Loaded, inactive	6.8	0.0%
Loaded, FAM active	7.0	2.2%
— + write monitoring	7.1	4.4%
— + — + read monitoring	7.1	4.4%
— + — + — + on-demand scan	9.6	41.2%
NLM unloaded	6.8	0.0%

Technical Details

Product: *Dr Solomon's Anti-Virus Toolkit for NetWare v7.72.*

Developer/Vendor: *Dr Solomons' Software Ltd*, Alton House, Gatehouse Way, Aylesbury, Buckinghamshire HP19 3XU, UK. Tel +44 1296 318700, fax +44 1296 318734, email support@drsolomon.com, WWW http://www.drsolomon.com/.

UK Price: £399 for a single server. Corporate and site licences, combining server and workstation products, should be discussed with a *Dr Solomon's* sales representative.

Hardware Used: Server: *Compaq* Prolinea 590, 80 MB RAM, 2 GB disk, *NetWare* 3.12. Workstation: *Compaq* DeskPro XE 466, 16 MB RAM, 207 MB disk, DOS 6.22, Windows 3.1.

[1]Test-sets: The test-sets used in this review are detailed on p.16 of this issue.

VB'97 – *The* Anti-virus Conference

The *Virus Bulletin* international conference is now in its seventh year. This annual conference is recognized as the world's leading event addressing the computer virus threat. *VB'97* will run as two parallel tracks, one corporate and one technical, and is being held at The Fairmont Hotel, San Francisco, USA on 2/3 October 1997.

Over three hundred delegates are expected to attend the presentations, which will be led by a panel of internationally renowned virus experts. The *VB'97* exhibition, featuring the world's leading anti-virus vendors, will run alongside the conference programme. Exhibitors include *McAfee*, *Dr Solomon's Software*, *Sophos*, *Command Software*, *NCSA*, *IBM*, *Integralis*, *Trend*, *Data Fellows*, and *Elsevier Science*.

The conference provides delegates with good opportunities to meet the industry experts and speakers. The social programme includes a welcome drinks reception and the spectacular black tie Gala Dinner. An interesting partners' program is available for delegates' partners and/or family.

If you would like further information on *VB'97*, please contact Alie Hothersall at *VB* (email alie@virusbtn.com) or visit the *Virus Bulletin* web site; http://www.virusbtn.com/.

PRODUCT REVIEW 2

AntiVirus Plus for Windows 95

Dr Keith Jackson

AntiVirus Plus from *Iris Software* claims to be 'a powerful protection tool that will stop electronic viruses from damaging your computer system'. The version provided for review comprised just two components – a stand-alone scanner, and a memory-resident software module.

I have reviewed *AntiVirus Plus* twice before for *VB*; in the January 1990 and December 1992 issues. This review only covers the *Windows 95* version of *AntiVirus Plus*, and does not look at any of its network-aware features.

Installation

AntiVirus Plus was provided for review as a set of two 1.44 MB, 3.5-inch floppy disks. These were not full-release disks as they had handwritten labels, and no documentation was included (apart from the on-line *Windows* help files).

Installation proved to be a doddle. A large ZIP file was copied from the floppy disk into a temporary sub-directory, the files within it extracted, and SETUP32.EXE executed. The on-screen 'Help' proved to be very good at explaining the various types of installation that were possible.

I was offered a choice between installing either the scanner and the 'Active Monitor' (memory-resident software), or just the scanner. I chose the former. After specifying the sub-directory to hold the *AntiVirus Plus* files, installation proceeded apace. The usual 'pretty pretty' *Windows* screens were displayed to keep the punters happy, and eventually I was asked to insert a floppy disk so that a 'Rescue Disk' could be created.

Making a Rescue Disk has a minor bug. If you do not insert a floppy disk when the installation program requests it, a dialog box containing only a single '!' appears. Initially I thought that the installation program was trying to tell me to wait while it copied files, but it slowly dawned on me that somebody had omitted the warning text. This is minor, but it is confusing and needs fixing.

The first of several easy-to-follow configuration dialogs.

As a finale, the installation offered to display the current README file, and then cautioned that the *AntiVirus Plus* features would not be active until the computer had been rebooted. After installation was finished, 25 objects had been installed, occupying a total of 3.26 MB of disk space.

Documentation

As I mentioned previously, *AntiVirus Plus* arrived for review without any physical documentation, so 'nought out of ten' for that part of the product. That said, the *Windows* help files are very clear, having been prettied up with lots of icons and pictures, and do give the basic details. However, they are very sparse on detail, so if anything really does go badly wrong, you have no choice but to telephone technical support.

The first time I reviewed *AntiVirus Plus*, I described the documentation as 'appalling'. Next time round it was summarized as 'not much better'. Indeed, the final sentence of that review was 'the content of the manual needs drastically extending and improving'. The problem has been solved in this latest incarnation – there is no documentation!

Speed

Using its default settings, *AntiVirus Plus* scanned the C: drive of my test PC in 54 seconds. This scan time stayed essentially the same when the log was deactivated, and when a 'Secure Scan' was used. However, the scan time reduced to just 34 seconds when a 'Fast Scan' inspecting only COM, EXE and OVL files was initiated.

It is interesting that creation of a log file has no measurable effect on the scan time *per se*. Note also that the default is to scan all files – most scanners do not bother to do this, and the developers of *AntiVirus Plus* are to be applauded at putting security before scan speed on this occasion.

For comparison purposes, the DOS version of *Dr. Solomon's Anti-Virus Toolkit* took 50 seconds, and the DOS version of *SWEEP* from *Sophos* 69 seconds, to perform the same scan. Therefore, the scanning speed provided by *AntiVirus Plus* is quite acceptable, up with the market leaders. However, this good result is rather marred when large numbers of viruses are found. Read on.

Scanning of Large Test-sets

I tested *AntiVirus Plus'* scanning capabilities by activating a scan of a CD-ROM containing the entire *VB* test-set (see Technical Details below for a list of which viruses are

currently used for testing purposes). *AntiVirus Plus* started scanning through the files quite efficiently, noting which files were infected, and creating a voluminous log file of what it had found.

Two days later it was still running… on a 133 MHz Pentium!

That is not a misprint, it really does say two days. Although *AntiVirus Plus* started off very efficiently, whizzing through the test files, beyond a certain point it slowed down to an interminable crawl, where it was taking more than two minutes to check each file.

I originally thought that this was due to very slow testing of the polymorphic test files, but the same thing happened when the 'Standard' test-set was tested last. Therefore, the slow-down is associated with the sheer volume of viruses being tested, not with any specific type.

As a humorous aside, when *AntiVirus Plus* did eventually finish its scan, the log file created by this long, long test stated that it had been scanning for just 3 hours 13 minutes 40 seconds. In reality, it had been scanning for this length of time plus two days. The log file has no means of reporting a scan time measured in days.

Scanning Results

AntiVirus Plus detected all bar one of the 476 samples contained in the 'In the Wild' file test-set. It only failed to detect one of the two samples of the No_Frills.Dudley virus. Not bad, close to perfect.

AntiVirus Plus detected only 523 of the 532 samples of the 'Standard' test set (98%). It missed nine test samples – both samples of Cruncher, one of three samples of Greets.3000, all three samples of Maresme.1062, both samples of Positron, and one of the six samples of the Yankee Doodle virus. All in all, this is also a quite acceptable result.

Indicative of things to come, *AntiVirus Plus* produced some interesting results scanning the In the Wild Boot test-set. With the Active Monitor disabled, the scanner detected all 91 boot viruses. With the Active Monitor enabled, however, accessing all the infected diskettes through *Windows'* Explorer resulted in three misses – Michelangelo.A, Misis, and Stoned.Daniela. This also happened when running a DOS 'dir a:' against the test-set; the Active Monitor also failed to find these three viruses in this situation. [*This is a manifestation of 'the BPB problem' referred to in the NT comparative,* VB *October 1996, p.12. Ed.*]

The polymorphic test-set currently contains 11,000 viruses (500 samples of 22 viruses, see Technical Details section below). *AntiVirus Plus* detected these polymorphic viruses nigh on perfectly (500 out of 500). The only polymorphs that it failed to detect were Girafe:TPE (which was not detected at all), and DSCE.Demo (where only seventeen out of 500 samples were detected). Therefore, overall, the polymorphic detection of *AntiVirus Plus* was 10,483 out of 11,000 (95.3%). Again, this is a very acceptable result.

None of the above results improved when the scanner was switched from the default setting of 'Fast Scan' to 'Secure Scan'. A 'Secure' scan is one where all parts of a file are tested for viruses, and a 'Fast' scan is defined by *AntiVirus Plus* as being one where 'specific parts of the files' are scanned. The help files state that *AntiVirus Plus* uses 'a special algorithm to decide' what these specific parts are. Special? Is that it for an explanation? Hidden more like, certainly I haven't a clue what a 'Fast scan' actually is.

Overall, the virus detection rate of *AntiVirus Plus* must be rated as good by any reasonable standard.

False Positives

I tested *AntiVirus Plus* against the *VB* false positive test-set. This comprises 5500 executable files, held on CD-ROM, all of which have been copied from well-known software products. Interestingly, *AntiVirus Plus* did come up with two false positives.

It thought that a program called INSTALL.COM (I don't know which product this executable was culled from) was infected by the OHBABY virus, and that a program called VIEW.EXE was infected with the 14366.VXE virus. The *AntiVirus Plus* scanner stated that neither of these viruses could be disinfected. This makes only two false positives from 5500 files, but any false positive whatsoever is a thorough nuisance.

This is the first product that I have reviewed in a long time to produce false positives. It would be interesting to know if *AntiVirus Plus* uses any heuristic methods during virus detection. This is often the cause of false positives. The help files are silent on this point.

Memory-resident Software

AntiVirus Plus incorporates memory-resident software called WIMMUN32 (a catchy little name if ever there was one). This software is automatically loaded and activated at boot time. In contrast to most other products that are on the market today, there is no way to configure the action of this memory-resident software, or if there is I could not find it. Although this makes it idiot-proof, it also makes it impossible to overcome any problems that may be encountered.

The *AntiVirus Plus* memory-resident software inspects executable code, checking that none of the thousands of virus signatures which it knows is present. If a virus is detected, then the program is prevented from executing, and a dialog box pops up over whatever application is running to warn that a virus has been detected. It also protects DOS applications running under *Windows 95*.

Measuring the detection rate of the *AntiVirus Plus* memory-resident software threw up some odd results.

For instance, clicking on the sub-directory that contained 'In the Wild' test-set viruses whose names commence with the letters 'A' through 'L', detected 98 viruses. However, if

Some of *AntiVirus Plus'* advanced configuration options.

these viruses were copied to another sub-directory, then 113 viruses were detected. So why are these two figures different? The memory-resident software must be using slightly different detection techniques in both cases.

For 'In the Wild' test-set viruses whose names begin with the letters 'M' through 'Z', *AntiVirus Plus* detected 109 viruses, but when I tried to copy these viruses to another sub-directory, the memory-resident software produced an error, and would not let me copy the files. I have no idea why there is a difference between the above two cases.

This means that, at best, 222 of the 476 samples of the 'In the Wild' test-set were detected by the memory-resident software. Nowhere near as good as the *AntiVirus Plus* scanner. By comparison, only 166 of the 532 samples contained in the 'Standard' test-set were detected by *AntiVirus Plus* memory-resident software. This is just 31%, and frankly that is not good enough.

One odd effect of the memory-resident software showed up when the 'Recycle Bin' was being cleared. If the 'Delete' option was selected after a virus had been detected, a warning message sometimes (rarely) popped up to say that an infected file had been found. This effect was indeed 'rare', it showed itself just three times for the 908 files contained in the 'In The Wild' and the 'Standard' test-sets. I have no idea why *AntiVirus Plus* should sometimes detect a virus whilst the Recycle Bin is being cleared.

The Rest

There are a myriad of options for tailoring *AntiVirus Plus*. These options refer to how the results are interpreted (what to do when a virus is found), and how to present the report files, rather than how to detect viruses *per se*. As far as detection goes, the options are 'Fast scan' or 'Secure scan'; and as the above measurements show, this does not really make much difference.

AntiVirus Plus makes grandiose claims that it 'literally *cures* your system of viruses'. Indeed, early versions of this software were called CURE, and the subtitle of the scanner is 'Cure for Windows'. However, virus disinfection is very dubious at best, and in many cases the virus destroys part of the original file, making disinfection impossible. I have always refused to review such features, and this product is no exception. Use a backup; you know it makes sense.

Conclusions

The problems that I encountered with large virus test-sets would not trouble the average user who will have just a few – at worst several hundred – infected files. However, *Iris Software* would be advised to look into the reason for the dramatic slowdown in virus detection.

The memory-resident software provided with *AntiVirus Plus* is not particularly good at detecting viruses. The results are somewhat confusing, but no matter how they are viewed, they can never match up to the claim made by the *AntiVirus Plus* developers that the memory-resident software can 'stop any known virus before it becomes active'. That is tosh; pure tosh. The marketroids may quibble, but missing about 50% of the 'In the Wild' test-set cannot be defined as stopping 'any known virus'.

Any anti-virus developer would be proud of the detection figures quoted above. The only glitch was a failure to detect one of the polymorphic viruses. If you want anti-virus software that is very capable of scanning for viruses, then *AntiVirus Plus* is not a bad buy.

Editor's note: Since preparing this review, Iris Software *informed us it sent a beta version for testing and insisted we re-test their released product.* Iris *has fixed the slow-down in scanning large virus sets.Despite claims to have corrected the false alerts problem, the update detected seven 'viruses' in our Clean set. The claim that the on-access scanner should now detect all viruses the on-demand one does was partly substantiated – the update detected all but 28 of the samples in the In the Wild File, Macro and Standard test-sets.* Iris *stresses that its product is mainly sold through OEM channels and via the WWW so there are no printed manuals.*

Technical Details

Product: *AntiVirus Plus.*

Vendor: *Iris Software*, 1173A 2nd Ave Suite 316, New York, NY 10021, USA, US Tel 1 800 947 4798, Tel from outside the USA +1 805 241 8775, email 102212,3026 on Compuserve or support@iris.co.il, WWW http://www.irisav.com.

Availability: IBM-PC or Compatible, running *Windows 95.*

Version evaluated: 22.0

Price: $19.95; 1 year upgrade subscription $9.95. Site and 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 operate under *Windows 95*, *Windows 3.11*, *Windows 3.1*, or DOS 6.22

Viruses used for testing purposes: Complete listings of the In the Wild File, Polymorphic and Standard test-sets used for this review can be found in *VB*, March 1997 p.17. The In the Wild Boot test-set is fully listed on p.16 of this issue.

SUBSCRIPTION RATES

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

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

Editorial enquiries, subscription enquiries, orders and payments:

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

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

US subscriptions only:

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

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

END NOTES AND NEWS

The **International Conference on Forensic Computing** will be held in Brighton from 3-5 December 1997. The event will feature more than sixteen speakers covering topics from evidence recovery and analysis techniques to computer forensics methodology and criminal case studies. For further information contact *The International Journal of Forensic Computing*; Tel +44 1903 209226, or email ijfc@pavilion.co.uk.

Precise Publishing announces the release of *Indelible DNA*, a program **which creates a unique, encrypted, identification code**. This code – said to be undetectable – is 'sprayed' across PCs, and is virtually impossible to remove. UK police are being issued with 'Clue' disks which decode the DNA and identify the owners of stolen computers. Cost; £19.95. Contact; Tel +44 1384 560527.

***CompSec 97* will be held in London** from 5–7 November 1997. The conference aims to help highlight the risk to IT systems, assess security shortcomings, and protect against fraud, disaster, and negligence. Information is available from Amy Richardson at *Elsevier Science*; Tel +44 1865 843643, fax +44 1865 843958, or email a.richardson@elsevier.co.uk.

Integralis temporarily joins forces with IT and intellectual property law specialists *Cole and Cole* to hold a series of seminars highlighting **the legal implications of inadequate IT security**. They will take place on 16 September at the Holiday Inn in West Drayton, and on 4 November at Butcher's Hall, both in London. To reserve a place, contact Lorna Steel; Tel +44 118 930 6060.

The **7th Annual Virus Bulletin Conference** takes place in San Francisco's Fairmont Hotel on 2/3 October 1997. *VB'97* is *the* anti-virus conference to be seen at in 1997. For more details, refer to p.20 of this issue or http://www.virusbtn.com/.

The **20th National Information Systems Security Conference** is being held from **7–10 October 1997** at the Baltimore Convention Center, Maryland, USA. Covering such critical IT issues as secure electronic commerce, Internet security, and virus detection, the conference attracts more than 2000 participants. For more information, visit the conference's Web site at http://csrc.nist.gov/nissc/, Tel +1 410 850 0272, or email NISSConference@dockmaster.ncsc.mil.

A **security product from *Priority Data* led to a criminal conviction** in July 1997. Encrypted data proving identification and ownership was extracted from a stolen laptop's hard disk and decoded by the previously installed *PD Secure*. Further information is available from the company's World Wide Web site at http://www.prioritydata.ie/.

The **Secure Computing Tactical Conference**, set for 7–9 October 1997, has been tactically re-scheduled until sometime possibly in February 1998. For more information, contact Norman Bullen; Tel +44 1792 324000, email nbullen@westcoast.com, or visit their Web site; http://www.westcoast.com/.

***Sophos Plc* is holding two computer virus workshops** this month at its training suite in Abingdon, UK, with an introductory course followed by an advanced one, on 24 and 25 September respectively. They are also hosting *Practical NetWare Security* courses on 9 September and 13 November. These one-day workshops cost £325+VAT, which includes a complimentary copy of *Sweep* for *Novell NetWare*. Contact Karen Richardson: Tel +44 1235 544015, fax +44 1235 55935, or see http://www.sophos.com/.

***Quarterdeck Corp* enters the anti-virus market** with the launch of *ViruSweep*, based on technology licensed from *EliaShim*. David Stang, formerly *NCSA*, is head of *Quarterdeck's* anti-virus research centre. More details on the WWW at http://www.quarterdeck.com/quarc/.