EDITORIAL

Windows NT: The OS for Generation X 2

VIRUS PREVALENCE TABLE 3

NEWS
1. Sexy Boza? 3
2. Stop Press: Irina 3
3. VB ’96 3

IBM PC VIRUSES (UPDATE) 4

VIRUS ANALYSIS
Cracking the Crackers 6

COMPARATIVE REVIEW
NT: The Next Generation? 8

PRODUCT REVIEWS
1. F-PROT Professional for Windows NT 18
2. A Product with Integrity 21

END NOTES & NEWS 24
EDITORIAL

Windows NT: The OS for Generation X

One of my most peculiar childhood memories revolves around having to wear the most extraordinar-
ily outsize clothes. It’s a strange thing, but there it is. My mother could often be heard uttering a
kind of mantra: ‘Oh, he’ll grow into it’. It seemed bizarre to me at the time, possessed as I was with
that curious logic children have; now, of course, that I’m relatively grown up, it makes perfect sense.

It’s a generally recurring theme, actually – buying things larger than you need them in anticipation
of ‘growing into them’. And now that I’ve actually gone out and asked, what should have been
obvious is made clear – everyone else’s parents did this to them as well. And it seems that the
parents did the right thing; we did indeed grow into the clothes, and it was cheaper in the long run.
However, for the seemingly endless months it took to grow, we looked slightly silly.

And so it has been with Windows NT, an operating system which has been waiting over two years
for hardware to catch up with it. Microsoft must have been spending the time looking at computers,
pursing their corporate lips, and saying ‘Oh, they’ll grow into it’. All this time, Windows NT has
been looking peculiar as users have struggled to run it on 486s with 16MB of memory, as they
fought to fit its vast number of files onto paltry little hard drives with less than half a Gigabyte of
space, and as they complained bitterly about its poor performance as a workstation operating system
when compared to the unstable, insecure, thoroughly inelegant, but considerably faster,
Windows 3.1.

To be fair to Microsoft, their baby has been on a serious diet: the bloated monstrosity which was
NT 3.1 had slimmed down considerably by the age of 3.5, and by the time it had become 3.51, it was
so much smaller that one review published at the time even called it ‘svelte’. Nonetheless, it is the
remarkable increase in the ‘average’ level of hardware (how anyone can ever claim to be able to
work out the average level of computer hardware I’ll never know) that has really made the differ-
ence. The clothes finally fit; NT has come of age.

In the same way that corporates are said to be holding off from Windows 95 until they can check out
Windows NT 4.0, friends who visit many companies in the course of their work report that a surpris-
ingly large number of corporates which are currently using NetWare 3, and are in a position to
expand to NetWare 4, are also stalling. They want to look at NT as well. Microsoft finds itself with
NT attacking both ends of the market: on the workstation side, it will take huge lumps out of 95’s
market, and as for the servers… well, isn’t it the logical choice with 95 on the clients?

However, fear not: these opinions are shared by the manufacturers of the NT anti-virus products I
tested recently (the results of these tests are published in this issue; see p.8). They are all too aware,
it appears, of the importance of turning out a slick NT product – the level of investment in anti-virus
software for Windows NT products is unprecedented; never before has one operating system been
regarded as presenting so much of a make-or-break opportunity to the manufacturers.

Although it is not quite yet a case of ‘will the last NetWare user please turn out the lights’, any
company which does not produce an NT anti-virus solution which is, at the very least, equal to their
NetWare offering will probably find themselves in dire straits before too long.

Producing a decent NT product is not a question of a simple port job, although a port can act as a
stop-gap – almost every company will get to their final product via a quick and dirty port of what-
ever they have for Windows 3.1 or Windows 95. However, customers should not settle for this type
of half-way house for too long, not with so many possibilities for elegant solutions and useful
features just waiting to be implemented. In addition, of course, competitors will be there, champing
at the bit to sell their brand-new, all-singing, all-dancing, NT protection system.

The computer-using community has finally caught up with NT: all types of software manufacturer,
not just those involved in anti-virus software, should by now be running at full pelt to catch them.
After all, it’d be terrible to get left behind, wouldn’t it?
**NEWS**

**Sexy Boza?**

On 14 September 1996, a file infected with a variant of the Boza virus was posted to numerous sex-related Internet newsgroups. The relevant messages, posted by a user masquerading as love@your.kid, contain a UUENCODEd file which, when extracted, produces a file called SEX.EXE or SEXY.EXE. This file contains Boza.c, the version of the virus published in [VLAD magazine](#) in February 1996, p.15]. The subject lines of the offending messages are:

- Great FTP listing - sex.exe [01/01]
- Child sex jpg's and info where to get it. - sexy.zip [01/01]
- Child sex ftp listing - sex.exe [01/01]

This variant is not really a virus – it is labelled as 'intended' by anti-virus researchers, meaning it is supposed to be a virus, but does not replicate. However, it is likely that the intended virus will do damage files it attempts to infect.

It is interesting to note the nature of the newsgroups targeted: again, as with Kaos4 in July 1994 (alt.binaries.pictures.erotica) and, more recently, Hare (alt.sex, although Hare was also posted to other, non-sex-related, groups), the sender has specifically selected newsgroups which users will usually be reluctant to admit to reading. The aim is clearly to make it difficult to establish a source for the infection.

The culprit has not yet been identified, but examination of the message headers seems to indicate a user of tiac.net, an ISP called The Internet Access Company in north-east USA.

**Stop Press: Irina**

*VB* has received information about a supposedly dangerous virus, Irina, which spreads through the Internet: the rumours started with a press release from [Penguin Books](#), publicising the imminent launch of an interactive novel written by Stephen Baxter, *Irina*, which is set on the World-Wide Web.

Guy Gadney, *Penguin*’s project manager for the novel, stated: ‘We are keen to quash the rumours about this supposed virus: the publicity material we sent out was in two parts, the second of which stated quite clearly that *Irina* was not, and had nothing to do with, a virus. By this time, the damage had been done.’ *VB* readers are advised to ignore any messages they receive warning them of the virus.

**VB ’96**

As the October issue of *Virus Bulletin* goes to proof, staff are congregating in Brighton to prepare for the annual *Virus Bulletin* conference. A full report on the proceedings will appear in the next edition, and readers are reminded that the 1996 proceedings are now available; price £50 + p&p, from *VB* offices.

---

**Prevalence Table – August 1996**

<table>
<thead>
<tr>
<th>Virus Type</th>
<th>Incidents</th>
<th>Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept</td>
<td>Macro</td>
<td>46</td>
</tr>
<tr>
<td>Form</td>
<td>Boot</td>
<td>29</td>
</tr>
<tr>
<td>AntiEXE.A</td>
<td>Boot</td>
<td>20</td>
</tr>
<tr>
<td>Parity_Boot.B</td>
<td>Boot</td>
<td>15</td>
</tr>
<tr>
<td>Hare.7610</td>
<td>Multi</td>
<td>14</td>
</tr>
<tr>
<td>Junkie</td>
<td>Multi</td>
<td>13</td>
</tr>
<tr>
<td>Ripper</td>
<td>Boot</td>
<td>13</td>
</tr>
<tr>
<td>AntiCMOS.A</td>
<td>Boot</td>
<td>12</td>
</tr>
<tr>
<td>Empire.Monkey.B</td>
<td>Boot</td>
<td>11</td>
</tr>
<tr>
<td>NYB</td>
<td>Boot</td>
<td>8</td>
</tr>
<tr>
<td>Quandary</td>
<td>Boot</td>
<td>5</td>
</tr>
<tr>
<td>Sampo</td>
<td>Boot</td>
<td>5</td>
</tr>
<tr>
<td>Tentacle</td>
<td>File</td>
<td>5</td>
</tr>
<tr>
<td>WelcomB</td>
<td>Boot</td>
<td>5</td>
</tr>
<tr>
<td>Natas.4744</td>
<td>Multi</td>
<td>4</td>
</tr>
<tr>
<td>AntiCMOS.B</td>
<td>Boot</td>
<td>3</td>
</tr>
<tr>
<td>Burglar.1150</td>
<td>File</td>
<td>3</td>
</tr>
<tr>
<td>Empire.Monkey.B</td>
<td>Boot</td>
<td>3</td>
</tr>
<tr>
<td>EXEBug.A</td>
<td>Boot</td>
<td>3</td>
</tr>
<tr>
<td>Imposter</td>
<td>Macro</td>
<td>3</td>
</tr>
<tr>
<td>Unashamed</td>
<td>Boot</td>
<td>3</td>
</tr>
<tr>
<td>Edwin</td>
<td>Boot</td>
<td>2</td>
</tr>
<tr>
<td>Feint</td>
<td>Boot</td>
<td>2</td>
</tr>
<tr>
<td>Stealth_Boot.C</td>
<td>Boot</td>
<td>2</td>
</tr>
<tr>
<td>Stoned.Angelina</td>
<td>Boot</td>
<td>2</td>
</tr>
<tr>
<td>Stoned.Spirit</td>
<td>Boot</td>
<td>2</td>
</tr>
<tr>
<td>Stoned.Stonehenge</td>
<td>Boot</td>
<td>2</td>
</tr>
<tr>
<td>Telefonica</td>
<td>Multi</td>
<td>2</td>
</tr>
<tr>
<td>Wazzu</td>
<td>Macro</td>
<td>2</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td>27</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>266</td>
</tr>
</tbody>
</table>


**Correction**

Following the news story entitled ‘Pricey Ludwig’ in the September 1996 edition of *Virus Bulletin*, Eugene Spafford points out that the so-called ‘source code’ for the Internet Worm presented by Mark Ludwig is not in fact the complete original source, but a partial decompilation of the code created from the binary executable file; the distinction being that the full original code is commented more completely and contains sections of code which have been disabled.
The following is a list of updates and amendments to the Virus Bulletin Table of Known IBM PC Viruses as of 21 September 1996. Each entry consists of the virus name, its aliases (if any) and the virus type. This is followed by a short description (if available) and a 24-byte hexadecimal search pattern to detect the presence of the virus with a disk utility or a dedicated scanner which contains a user-updatable pattern library.

<table>
<thead>
<tr>
<th>Virus Name</th>
<th>Type</th>
<th>Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Queen.467</td>
<td>CER</td>
<td>E800 005D 81ED 0300 0E1F 06B4 ACCD 213C 3075 0B2E 3B9E CF01</td>
</tr>
<tr>
<td>Ambulance.2124</td>
<td>CER</td>
<td>B8FF DDCD 2180 FCCC 7507 3CC0 7203 E9CE 0088 0935 CD21 2E89</td>
</tr>
<tr>
<td>Antiwin.2320</td>
<td>ER</td>
<td>0500 0189 84AA FEB4 40B9 DE01 8B06 CD21 B800 4233 C933 D2CD</td>
</tr>
<tr>
<td>Baran.3294</td>
<td>CER</td>
<td>2E89 8414 08B8 0A08 03C6 A304 008C 0E06 080C 580D 0001 509D</td>
</tr>
<tr>
<td>Baran.4968</td>
<td>CER</td>
<td>2E8C 062C 02B8 FE48 CD21 3D01 FE75 4D90 2E89 1630 02FC 33C0</td>
</tr>
<tr>
<td>Creeper.478</td>
<td>CR</td>
<td>0500 0189 84AA FEB4 40B9 DE01 8B06 CD21 B800 4233 C933 D2CD</td>
</tr>
<tr>
<td>Gerd.798</td>
<td>CN</td>
<td>B440 881E 9005 BA92 05B9 1E03 90CD 21B4 3E8B 1E90 05CD 21C7</td>
</tr>
<tr>
<td>Holera.1488</td>
<td>CER</td>
<td>50B4 FECD 2158 B1FB 9619 7402 F9C3 F8C3 EEDE FF73 2750 5351</td>
</tr>
<tr>
<td>Httm.572</td>
<td>CR</td>
<td>50B4 FECD 2158 B1FB 9619 7402 F9C3 F8C3 EEDE FF73 2750 5351</td>
</tr>
<tr>
<td>Httm.580</td>
<td>CR</td>
<td>50B4 FECD 2158 B1FB 9619 7402 F9C3 F8C3 EEDE FF73 2750 5351</td>
</tr>
<tr>
<td>IVP.737</td>
<td>CEN</td>
<td>82DE 1601 B9B9 022E 8A27 2E32 A6E5 032E 8827 43E2 F2C3 ??</td>
</tr>
<tr>
<td>JTTP.3423</td>
<td>ER</td>
<td>B409 CD21 58E6 1A90 3D00 4B75 14E8 AC01 E846 0073 06E8 DE00</td>
</tr>
<tr>
<td>Nostardamus.3072</td>
<td>CER</td>
<td>B409 CD21 58E6 1A90 3D00 4B75 14E8 AC01 E846 0073 06E8 DE00</td>
</tr>
</tbody>
</table>
Konkoor.3072

ER: A preending, 3072-byte virus with plain-text messages: ‘Incorrect DOS version’ and ‘SCAN CLEAN VSHIELD FINDVIRU FV386 FV86 CLEANBOO VIVERIFY CERT MSAV GUARD TDUMP MKZ’ and the encrypted text: ‘Konkoor v2.0 - Crack Master - Last Days Of 1995 What Was The First Iranian Virus ? ! Abbas ??! (Was it Iranian ?) 2. Roohi 3. TDD - Konkoor v1.0 4. None Of Above =- This is The Last One If You Solve Copyright Problem =-Choose the correct answer...’. Infected files’ time stamps are set to 2 seconds.

Konkoor.3072

Nostardamus.3584

CER: A stealth, polymorphic, multi-copy encrypted, appending, 3584-byte virus containing the text: ‘a=Unlimited Grief=-’, ‘COMEXEVO/LOVPROSCHAEXTWEBARLRR/HAZIPCOMWINCHK’, ‘Kiev96’, ‘EMME 3’ and ‘Killer’. All infected files have their time-stamp set to 32 seconds. The following pattern detects the virus in memory only.

Nostardamus.3584

Salman.2000

EN: An encrypted, appending, 2000-byte virus containing the text: ‘*:exe’, ‘:\ chklist.ms chklist.cps cs\signature.dat SCAN.EXE CLEAN.EXE NAV.EXE EXEPACTRUN.EXE’, ‘Kill Salman Rushdie and Taslima Nasrin !’ and ‘Kill them !!!’.

Salman.2000

Shift.2010

CER: An appending, 2010-byte virus containing the text: ‘Your computer is infected by SHIFT VIRUS’ and ‘This virus is dedicated to PCC, and was written by a PCC student. ALEX’. The virus reinfeccts infected files.

Shift.2010

SillyComp.219

ENP: A simple, 219-byte companion virus which infects one file at a time, but only in subdirectories.

SillyComp.219

Tanpro.749

CER: A preending, 749-byte virus containing plain-text messages: ‘Screen Shaker 5th’ and ‘(c)tanpro’94’.

Tanpro.749

Teraz.2717

CER: An appending, 2717-byte virus which uses some anti-tracing tricks to hide itself in memory. It may reside above 640K. All infected files have their time-stamp set to 2 seconds.

Teraz.2717

Timish.2132

CER: An encrypted, preending (COM) and appending (EXE), 2132-byte virus containing the text: ‘commandcomexe’ and ‘Greetings from Timishtoara ! Call 040-61-13821’ (the latter displayed inside a double frame).

Timish.2132

Tucuman.828

ER: An appending, 828-byte virus containing the plain-text message: ‘UTN-FRT Tucumán, Argentina by Mr. Bithead - 1995’. All infected files have their time-stamp set to 32 seconds.

Tucuman.828

V.1468

CER: A stealth, appending, 1468-byte virus. While infecting COMMAND.COM the virus overwrites the last 1468 bytes (which are usually filled with zeros). All infected files have their time-stamp set to 62 seconds. The virus can be detected using a template for the V.1458 virus [see VB, June 1996].

VCL.523

CN: An encrypted, appending, 523-byte, direct infecter containing the text: ‘*.* *.COM’ and ‘[VCL]’.

VCL.523

Werewolf.678

EN: An encrypted, 678-byte, direct infecter containing the text: ‘Home Sweap Home (C)1994-95 WereWolf’ and ‘*:MS * CPS ANT*DAT’.

Werewolf.678

Werewolf.1152

CER: A stealth, appending, 1152-byte virus containing the text: ‘SCREAM! (C)1996 WereWolf’ and ‘CLEAN AVP TB V SCAN NAV IBM FINDV GUARD FV CHKDS F-’.

Werewolf.1152

Werewolf.1168

CER: A stealth, appending, 1168-byte virus containing the text: ‘SCREAM! (C)1995-96 WereWolf’ and ‘CLEAN AVP TB V SCAN NAV IBM FINDV GUARD FV CHKDS F-’.

Werewolf.1168

WhiteLion.942

CER: An appending, 942-byte virus containing the encrypted text: ‘WHITE LION Silent warrior in the jungle of softwares’.

WhiteLion.942

Xuxa.1984

CER: A stealth, encrypted, 1984-byte virus containing the text: ‘XUXA PARK 2.0 ■ By Hades ■ Todo el mundo esta feliz ?’, ‘TBF-ZIRJCHKCHKLIST.MS’, ‘ANTI-VIR.DAT’ and ‘COMEXE’. All infected files have their time-stamp set to 38 seconds.

Xuxa.1984

Zibbert.1268

CER: An appending, 1268-byte virus containing the text: ‘:\COMMAND.COM \COMMAND.COM’. Starting from July, on every Tuesday and Thursday, characters ‘a’ and ‘A’ are replaced with spaces when sent to a printer.

Zibbert.1268

Zibbert.1315

CER: An appending, 1315-byte variant of the above virus.

Zibbert.1315
Cracking the Crackers
Eugene Kaspersky

The Nutcracker story continues apace: the author of this particular family of viruses is still hard at work. Despite the fact that he is under investigation by the authorities, more and more new creations appear, all signed by Nutcracker. We can only hope that he suffers the same fate as that which befell the Black Baron.

A README.TXT file, in which the author promises not to release any more new viruses, comes with some of the viruses I have seen from this family. He never keeps his word, however, and new variants of Nutcracker appear amazingly quickly.

Created in several styles, called Nutcracker.ABn, each of the viruses contains something new. AB1 and AB2 both have new polymorphic engines and a new infection technique which makes disinfection of infected files extremely difficult. At present, seventeen distinct AB2 viruses are known!

Other family members have new stealth algorithms and any number of other tricks; all described in VB, February 1996, p.9. Three viruses in yet another style appeared a couple of months ago: AB0, dangerous, memory-resident, stealth, boot sector viruses.

New Techniques

Most boot viruses hook Int 13h or Int 40h to intercept disk access requests and to enable their infection and stealth routines to receive control and do their work. The exception is Nutcracker.AB0; it uses Int 15h instead.

On standard AT and PS systems, the BIOS Int 13h handler contains a call to Int 15h, AX=9000h/9100h, and the Int 40h handler contains a call to Int 15h, AX=9001h/9101h. These are called, respectively, the Device Busy and Device Post calls and signify that the BIOS is performing a read/write operation on a disk. Multi-tasking systems can then hook these to allow other tasks to execute whilst the I/O request is completed.

The virus makes use of this PC feature by hooking Int 15h. It will therefore receive control whenever the disks are accessed: first the system will call Int 13h, which itself issues an Int 15h which has been hooked by the virus; then Nutcracker takes control.

On Disks

On a floppy disk, the virus occupies the boot sector and five sectors on the hidden track at the end of the diskette. When a system is booted from an infected diskette, the virus is loaded and run from the boot sector. It then reads the body of its code from the end of the floppy, and jumps into it. The original boot sector is then read to the standard boot code address (0000:7C00h), and control returns there when infection is complete.

The virus loads from hard disk in a fashion which, although slightly unusual, has been seen in previous virus analyses [see analysis of Hare; VB, August 1996, p.11]. When a Nutcracker virus infects a disk, it stores the body of its own code in an extra track at the end of the disk, and then modifies the Partition Table held in the MBR so that the active partition record (i.e. the partition from which the operating system, under normal circumstances, is loaded) points to this area.

Thus, it is not actually necessary for the virus to modify any of the code in the Master Boot Sector, merely the Partition Table stored there. Hence attempting to clean the virus with the traditional FDISK /MBR will have no effect, as this leaves the Partition Table intact.

Installation

When the body of the virus is executed, if it was loaded from a diskette, it first checks to see if the hard disk is already infected. It does this by examining the Partition Table to obtain the disk address of the boot sector of the active partition, which it then loads.

If the virus is already present on the disk, that sector will be the first of the virus body. Nutcracker compares 12 bytes of the sector with its own code to establish whether or not this is the case. If the hard disk is not already infected, Nutcracker then infects it.

The virus next hooks Int 08h (System Timer), Int 15h, and Int 40h (Relocated BIOS Diskette Handler). The technique of hooking Int 08h is a standard one, used by many viruses which need to watch the system to wait until DOS has loaded before hooking more interrupts – this is exactly what Nutcracker is doing. Once DOS is loaded, it hooks Int 15h and Int 21h.

The Int 21h hook is only temporary, and is used to allow the virus to move its TSR (Terminate and Stay Resident) code once DOS is loaded. It waits for the first call to Int 21h, AX=4B00h (Load and Execute): when it sees this, it...
allocates a block of system memory, moves the resident code there, corrects all of its interrupt hooks to point to the new copy, and finally releases Int 21h.

The memory allocation is performed with calls to the HMA memory manager. If HMA is available, memory is taken from that area; otherwise, it merges its newly-allocated block with the highest allocated block.

**Interrupts**

Nutcracker hooks Int 15h somewhat indirectly; it writes CD7Eh (a call to Int 7Eh) over the first two bytes of the Int 15h handler, and then hooks Int 7Eh.

This handler checks for four Int 15h functions – AX=9000h, 9001h, 9100h, and 9101h. When a matching call is made, the virus passes control to its infection and stealth routines as appropriate. In addition, if a write is made to the hard disk’s MBR, the virus immediately reinfests it.

The Int 40h handler is used to allow the virus to infect floppy diskettes when I/O requests are sent destined for one of the floppy drives.

**Infecting Disks**

Other than the details given above, there are still a couple of things to mention about infection. When the Nutcracker virus is about to infect a diskette, it hooks Int 1Eh; and when it is about to infect a hard disk, it hooks Int 76h (Hard Disk Controller Complete). The hook is released as soon as infection is complete.

In addition, the virus uses port-level access to hard disks in an attempt to avoid anti-virus detection.

**Triggers**

These Nutcracker viruses have several payloads – if a floppy disk is accessed when the system timer value ANDed with F07Fh is zero, the virus displays a bouncing ball on the screen (much like the PingPong virus).

In addition, the viruses use an Int 15h hook to monitor Int 15h, AH=4Fh (Keyboard Intercept). If Ctrl-Alt-Del is pressed whilst the bouncing ball is being displayed *after all, what else is a user likely to do when he sees a ping-pong ball on his screen? Ed.*, the virus may (depending on the system timer) erase sectors from the hard drive.

Nutcracker also monitors the system for programs writing the virus’ own code out to disk; if it spots such activity, and the program performing the writing is not the virus itself, it will erase sectors from the hard drive. Therefore, anti-virus researchers must be careful when experimenting with the virus, lest it destroy their work.

In addition, if a read error occurs whilst loading from an infected disk, or if the virus is already in memory, it decrypts and displays a message similar, but not identical to, the standard DOS error message:

```
Non-system disk or disk error. Replace and press strike any key when ready.
```

Finally, On 7 April, the virus decrypts and displays the following message:

```
_S_U_P_E_R_U_N_K_N_O_W_N_ was done by Lord Nutcracker(ABO).
```

**Nutcracker.AB0**

<table>
<thead>
<tr>
<th>Alias:</th>
<th>None known.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type:</td>
<td>Memory-resident boot infector with stealth functionality.</td>
</tr>
<tr>
<td>Infection:</td>
<td>Boot sectors of floppy disks; MBR of hard drive.</td>
</tr>
<tr>
<td>Self-recognition in Sectors:</td>
<td>Compares 12 bytes of its own code with the code in the sector.</td>
</tr>
<tr>
<td>Self-recognition in Memory:</td>
<td>Temporarily sets the byte at address 0000:0087 (address of Int 21h handler) to 7Bh, and then checks that byte whilst loading from an infected disk.</td>
</tr>
<tr>
<td>Hex Patterns in Sectors and in Memory:</td>
<td></td>
</tr>
<tr>
<td>Nutcracker.AB0.a and Nutcracker.AB0.c:</td>
<td></td>
</tr>
<tr>
<td>2BDB FA8E D3BC 007C 8EC4 FBB9</td>
<td></td>
</tr>
<tr>
<td>7411 BF03 002A E4CD 13B8 0502</td>
<td></td>
</tr>
<tr>
<td>CD13 730B 4F75 F2BE 8E7C E807</td>
<td></td>
</tr>
<tr>
<td>Nutcracker.AB0.b:</td>
<td></td>
</tr>
<tr>
<td>2BDB FA8E D3BC 007C 8EC4 FBB9</td>
<td></td>
</tr>
<tr>
<td>7411 BF03 002A E4CD 13B8 0502</td>
<td></td>
</tr>
<tr>
<td>CD13 730B 4F75 F2BE 487C E807 19EA 9700 007C</td>
<td></td>
</tr>
</tbody>
</table>

| Intercepts: | Int 08h, to hook other interrupts and call trigger routine. |
| Int 15h, to hook Int 13h and call infection and stealth routines. |
| Int 1Eh, temporarily, whilst infecting floppy disks. |
| Int 21h, temporarily, whilst infecting floppy disks. |
| Int 40h, to infect floppy disks. |
| Int 76h, temporarily whilst infecting the MBR. |

| Trigger: | Erases hard drive sectors, launches a PingPong-like jumping ball, and displays a message. See analysis for more details. |

| Removal: | Under clean system conditions, identify and replace infected floppy boot sectors, and fix the Partition Table in the MBR of the hard drive. |
COMPARATIVE REVIEW

NT: The Next Generation?

Windows NT is an operating system whose time has very definitely come – the average level of PC hardware is perfectly up to the task of running it, and many organisations are holding off from upgrading to Windows 95 until they’ve had the chance fully to evaluate NT 4.0, the latest version of Windows NT. The corporate prices of the two are not that dissimilar, nor are the hardware requirements.

However, at this point in time, the major use for Windows NT is as a server operating system – it has been making inroads into the market domination of Novell’s NetWare. It offers easy scalability to platforms other than Intel-based PCs – if your network outgrows your Pentium server, why not upgrade it to a DEC Alpha?

Newfangled Testing

Not all that long ago, reviewing anti-virus products could be done adequately with a single 386 with a couple of MB of memory, a tiny hard disk, a VGA monitor, and some out-dated 90MB Bernoulli disks. Those days are gone. I once ran Windows NT on a 386/25 with 10MB of memory and a slow 80MB hard disk, but after therapy I have almost managed to block it from my mind – it is not an experience I want to repeat.

The system used for this review was of a higher specification: readers should refer to the Technical Details at the end of the review. Windows NT Server 3.51 (the shipping version at the time the products were submitted) was used, and Service Pack Four was applied. The network used consisted of the NT server, a NetWare 3.12 server, and three DOS clients. This allowed testing of most aspects of product functionality.

Testing

The test-sets have expanded since the last comparative, in July 1996 – the In the Wild file and Boot Sector sets have been brought up to date with the June WildList, and include all viruses from the top section of the list which could be replicated. The Standard test-set has been expanded, but the Polymorphic set remains unchanged from the July review.

It was also decided, following that comparative, to run the products in a mode such that they scan all files, rather than just those which match a product’s default extension list. This is done because there is no requirement that documents are named .DOC.

The make-up of the speed sets is listed in the Technical Details section at the end of the review; all products are run on a fresh installation of Windows NT with no other software running apart from Program Manager. As Windows NT is an operating system which is fully multi-tasking, it can be difficult to reproduce speed figures unless great care is taken. In all cases, the anti-virus product was the foreground application, and the system’s tasking configuration was set to the default, ‘Best Foreground Application Response Time’. Tests were performed immediately following a reboot.

Also in the Technical Details section is a WWW address for a document describing in detail the calculation system used. This lays out the entire system in more depth than is possible in the pages of VB, and includes worked examples.

Resident Software

Only four of the products submitted – those from Cheyenne, Intel, McAfee, and S&S – were supplied with on-access components. These parts of the products were not tested to the same extent as the conventional scanner; however, they were tested for basic functionality – to ensure that they detected files opened and executed, and boot sectors on floppy disks accessed, and that files on all types of filing system (local and remote) were checked.

The final test was to stress the on-access scanner on the server for several hours, continually opening and closing files both on the server itself and from client machines in a basic attempt to provoke some form of slip on the part of the software. Performance Monitor was used to check for memory leaks after this test.

Alwil AVAST! (Build 349)

<table>
<thead>
<tr>
<th>Test</th>
<th>Score</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot</td>
<td>100.0%</td>
<td>Standard 100.0%</td>
</tr>
<tr>
<td>File</td>
<td>100.0%</td>
<td>Polymorphic 100.0%</td>
</tr>
<tr>
<td>Overall</td>
<td>100.0%</td>
<td></td>
</tr>
</tbody>
</table>

This Czech product continues to go from strength to strength: the most obvious thing to say here is that it found all the test viruses. Every one. Impressive, to say the least.

On other fronts, the product’s front-end is… well, different. There is liberal (even over-enthusiastic) use of expandable list selectors: in tandem with a non-resizable base window, this makes things difficult to use. Rather than presenting the user with the more conventional list of drives and offering to scan them, if the user wishes to scan a particular object or group of objects, he must create a new job. The user is introduced quickly to the fairly advanced concept of creating and
The product presents itself as an MDI, with three main windows: the Domain Manager, the Service Manager, and the Local Scanner. The simplest, the Local Scanner, allows selection and scanning of local drives and visible network drives and their directories. The usual options are available, but a scan configuration cannot be saved for use in the next session. Information and reports from previous scans can be examined and manipulated as desired.

The Service and Domain Manager dialogs are somewhat confusing – the Domain Manager allows the user to examine a ‘Summary View’ of the InocuLAN machines on the network, which is extraordinarily similar to the view presented by the Service Manager, although identical icons (a red square and a green arrow) on the toolbars of the respective windows have completely different effects. It is easy to become confused as to what is on view, hence to know what effect pressing a button will have. There was also evidently an error at installation – one of the help files was not available. The Domain Manager is more powerful – it allows viewing of relevant event log entries and reports from machines across the network, and scheduled jobs to be created, configured, and modified on any such machine. It also contains the controls for the real-time scanning component, which is configurable on a per-machine basis – the choice is between scanning files being placed onto the server, files being copied off the server, both, or neither. A user can also modify the extension list and the detection action.

In stress testing, the real-time scanner held up well, with no detectable memory instability over the period of the test. There was, however, a serious anomaly: when a session on the NT server accessed a file on the NetWare server, the monitor did not check it – a definite omission and hole in the protection.

The product does not disappoint. It is at the high end of the functionality range, offering sophisticated domain management features and real-time scanning, along with the expected scheduled and on-demand functionality.

Cheyenne InocuLAN (v1.01)

| IIW Boot | Standard | 97.5% |
| IIW File | Polymorphic | 97.2% |
| IIW Overall | | 97.4% |

One always expects both pretty and powerful things from Cheyenne: the current release of InocuLAN for Windows NT does not disappoint. It is at the high end of the functionality range, offering sophisticated domain management features.
Detection rates were good but not excellent: the product missed 100% In the Wild detection, failing to detect Chance.B and Pasta in the In the Wild Boot Sector set, and Ph33r.1332, Desperado.1403.C, and Major.1644 in the In the Wild File set. Scores in the other test-sets were good: the improvement we have come to expect from InocuLAN is continuing.

Cybec VET (v9.0.5)

In fairness, there is a 32-bit command-line scanner, which can be used in conjunction with NT’s built-in scheduling service. Running VET in this fashion, however, means it cannot check the boot sectors of the machine in question, leaving a fairly serious gap in protection.

The interface is easy to use, though different in style from many others in this review – the user is presented with a standard MDI in which he may view the drive/directory structure of the machine (the browser), and the report file for VET’s current session. Simple scanning is performed by selecting the drive, directory or file to be scanned, and clicking on the VET icon, or using the RHB context-sensitive menu. However, it is not clear why Windows Cut/Copy/Paste options are available on selected objects in the browser: pasting into the report window simply enters the filename, and into other Windows applications, had the same results.

As to scanning options, VET is different from the other products tested in that, when presented with an infected file, it disinfects it by default without confirmation from the user, and without creating a backup. This does have advantages (fewer decisions for users to make) but it requires placing a fair amount of trust in the developer’s ability to write disinfectors which work correctly every time. The action can be changed if desired.

VET is impressively quick: it was the fastest product in the floppy tests, but NAV beat it narrowly in the clean hard drive scan timings. As to detection, VET is above average; getting just under 100% on the In the Wild sets (missing Pasta and Stoned.Spirit on the In the Wild Boot sector set and Werewolf.1500.B, Desperado.1403.C, and a sample of Sayha on the ItW files). Combined with very creditable Standard and Polymorphic results, the final result gets better all the time.

DataFellows F-PROT Professional (v2.23)

F-PROT for NT’s heritage is clear – it is remarkably similar to F-PROT for Windows and for Windows 95 (even the icon reads ‘F-PROT Professional for Windows’). This said, the interface is perfectly usable, consisting of the traditional menu and button bars, beneath which is a task selection area. Tasks are created and modified using buttons beneath this area.

Any task listed can be scheduled to occur at any time, and to repeat at almost any interval: the Schedule dialog is positively alive with boxes to select. Unfortunately, scheduling is handled by a user-level application placed into the Startup group on installation, so scheduled scans do not fire if no-one is logged on. It is necessary to save the settings explicitly, or they will not take effect; also, there appears to be a bug in this area of the program, and saved tasks are lost between sessions, making scheduling something of a problem.
<table>
<thead>
<tr>
<th>Product</th>
<th>ItW Boot</th>
<th>Percent</th>
<th>ItW File</th>
<th>Percent</th>
<th>ItW Overall</th>
<th>Percent</th>
<th>Standard</th>
<th>Percent</th>
<th>Polymorphic</th>
<th>Percent</th>
<th>Number</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alwil AVAST!</td>
<td>80</td>
<td>100.0%</td>
<td>342</td>
<td>100.0%</td>
<td>100.0%</td>
<td>511</td>
<td>100.0%</td>
<td>8854</td>
<td>85.2%</td>
<td>9042</td>
<td>87.8%</td>
<td></td>
</tr>
<tr>
<td>Cheyenne InocuLAN</td>
<td>78</td>
<td>97.5%</td>
<td>332</td>
<td>97.2%</td>
<td>97.4%</td>
<td>431</td>
<td>91.1%</td>
<td>8555</td>
<td>50.4%</td>
<td>5553</td>
<td>98.3%</td>
<td></td>
</tr>
<tr>
<td>Cybec VET</td>
<td>78</td>
<td>97.5%</td>
<td>336</td>
<td>98.0%</td>
<td>97.8%</td>
<td>403</td>
<td>87.9%</td>
<td>9042</td>
<td>87.8%</td>
<td>9042</td>
<td>87.8%</td>
<td></td>
</tr>
<tr>
<td>DataFellows F-PROT</td>
<td>64</td>
<td>80.0%</td>
<td>342</td>
<td>100.0%</td>
<td>91.5%</td>
<td>446</td>
<td>92.3%</td>
<td>5553</td>
<td>50.4%</td>
<td>5553</td>
<td>50.4%</td>
<td></td>
</tr>
<tr>
<td>ESaSS ThunderBYTE</td>
<td>80</td>
<td>100.0%</td>
<td>332</td>
<td>97.5%</td>
<td>98.5%</td>
<td>477</td>
<td>95.8%</td>
<td>9943</td>
<td>98.3%</td>
<td>9943</td>
<td>98.3%</td>
<td></td>
</tr>
<tr>
<td>H+BEDV AntiVir</td>
<td>52</td>
<td>65.0%</td>
<td>227</td>
<td>70.6%</td>
<td>68.3%</td>
<td>230</td>
<td>63.2%</td>
<td>4504</td>
<td>45.0%</td>
<td>4504</td>
<td>45.0%</td>
<td></td>
</tr>
<tr>
<td>Intel LANDesk</td>
<td>60</td>
<td>75.0%</td>
<td>335</td>
<td>98.2%</td>
<td>88.4%</td>
<td>330</td>
<td>77.4%</td>
<td>8299</td>
<td>77.2%</td>
<td>8299</td>
<td>77.2%</td>
<td></td>
</tr>
<tr>
<td>McAfee NetShield</td>
<td>80</td>
<td>100.0%</td>
<td>332</td>
<td>97.7%</td>
<td>98.7%</td>
<td>439</td>
<td>91.2%</td>
<td>7303</td>
<td>67.3%</td>
<td>7303</td>
<td>67.3%</td>
<td></td>
</tr>
<tr>
<td>Norman Virus Control</td>
<td>80</td>
<td>100.0%</td>
<td>332</td>
<td>97.5%</td>
<td>98.5%</td>
<td>477</td>
<td>95.8%</td>
<td>9943</td>
<td>98.3%</td>
<td>9943</td>
<td>98.3%</td>
<td></td>
</tr>
<tr>
<td>S&amp;S Dr Solomon's AVTK</td>
<td>80</td>
<td>100.0%</td>
<td>342</td>
<td>100.0%</td>
<td>100.0%</td>
<td>509</td>
<td>99.6%</td>
<td>10000</td>
<td>100.0%</td>
<td>10000</td>
<td>100.0%</td>
<td></td>
</tr>
<tr>
<td>Sophos SWEEP</td>
<td>65</td>
<td>81.3%</td>
<td>342</td>
<td>100.0%</td>
<td>92.1%</td>
<td>505</td>
<td>99.2%</td>
<td>9498</td>
<td>93.7%</td>
<td>9498</td>
<td>93.7%</td>
<td></td>
</tr>
<tr>
<td>Stiller Integrity Master</td>
<td>0</td>
<td>0.0%</td>
<td>332</td>
<td>97.3%</td>
<td>56.1%</td>
<td>496</td>
<td>98.0%</td>
<td>4769</td>
<td>44.5%</td>
<td>4769</td>
<td>44.5%</td>
<td></td>
</tr>
<tr>
<td>Symantec Norton AV</td>
<td>80</td>
<td>100.0%</td>
<td>337</td>
<td>98.6%</td>
<td>99.2%</td>
<td>403</td>
<td>87.4%</td>
<td>5734</td>
<td>56.8%</td>
<td>5734</td>
<td>56.8%</td>
<td></td>
</tr>
</tbody>
</table>

The product has remote updating features which utilise a shared communication directory on the server, allowing clients to install updates when a new version is available – the solution is not as sophisticated as Cheyenne’s, but it works well, provided all machines access the same shared drive.

*F-PROT* is the first product described here to suffer from failure to detect boot sector viruses on diskettes not readable by the operating system [see *The BPB Problem, p.12*]. This failure damages the boot sector score quite severely. The In the Wild file score is perfect, as we have come to expect from this product.

**ESaSS ThunderBYTE (v7.04)**

<table>
<thead>
<tr>
<th>ItW Boot</th>
<th>100.0%</th>
<th>Standard</th>
<th>95.8%</th>
</tr>
</thead>
<tbody>
<tr>
<td>ItW File</td>
<td>97.5%</td>
<td>Polymorphic</td>
<td>98.3%</td>
</tr>
<tr>
<td>ItW Overall</td>
<td>98.5%</td>
<td>98.3%</td>
<td></td>
</tr>
</tbody>
</table>

This product bears a remarkable resemblance to another – *ESaSS* and *Norman* have a ‘strategic alliance’ [see VB, *May 1995, p.3*], which goes some way towards explaining why their products are so similar.

*ThunderBYTE for Windows NT (TBAVNT)* uses a drive-selection window beneath the expected button and menu bars; the only surprise comes when you notice the floating button bar. Mentioned in the *Norman* product’s section of the *Windows 95* comparative earlier this year [see VB, *June 1996, p.12*], this is a natty little idea, but a little too crowded and confusing for comfort.

The product uses ‘styles’ to save scan settings for repeated use, or for use as part of a scheduled scan configuration: these are administered adequately, if not, perhaps, entirely intuitively.

For example, this reviewer was expecting to be able to set up a scan manually and then save it as a style. This is not, however, the case: the configuration must be set up from within the style dialog, and it is not possible to ask it to scan only a certain subdirectory tree from a style, only drives and combinations of drives.

Scheduling is available on any defined style via the *TBAV* Scheduler, enabling a number of scans to trigger daily, weekly or monthly (the time granularity is 15 minutes). A user-level application performs scheduling, so the user must be logged on for the scan to take place.

*TBAV* is always mentioned in *Virus Bulletin DOS* comparative reviews as being very fast; however, *Windows NT* does not allow the type of low-level disk access that *TBAV* for *DOS* uses to give it such speed, hence the product is not as far ahead as usual. Nevertheless, it still manages to fall in the top half of the speed figures.

Detection is a respectable 98.5%: the product missed some samples of Imposter, and all those of Wazzu and Werewolf.1500.B. Polymorphic detection is very good indeed, as is to be expected from a product which ‘contains’ *Norman* technology.
**H+BEDV AntiVir (v1.07.4)**

<table>
<thead>
<tr>
<th>Category</th>
<th>percentage</th>
<th>Type</th>
<th>percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ItW Boot</td>
<td>65.0%</td>
<td>Standard</td>
<td>63.2%</td>
</tr>
<tr>
<td>ItW File</td>
<td>70.6%</td>
<td>Polymorphic</td>
<td>45.0%</td>
</tr>
<tr>
<td>ItW Overall</td>
<td>68.3%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*AntiVir* is the product of *H+BEDV*, a German company based near Lake Constance, close to the German/Austrian border. Its scanner has performed well in previous VB DOS scanner comparatives. *AntiVir for Windows NT* is a new product, only available in German; fortunately, *VB* boasts a German speaker.

The product is basic in functionality, offering the standard on-demand windowed scanner and scheduled scanner functionality – scheduling is provided by a user-mode application, meaning scans cannot be carried out without a user logged on, and the application running.

The scanner interface is a standard drive selection box, with buttons to select all the drives of the various types, and a button bar along the top of the window to allow various commonly-needed tasks to be run. Simple, but nonetheless functional.

Detection rates not nearly as good as could be hoped: just over 68% of ItW viruses detected is not sufficient to form adequate protection, and results in the other categories are equally uninspiring.

**Intel LANDesk Virus Protect**

<table>
<thead>
<tr>
<th>Category</th>
<th>percentage</th>
<th>Type</th>
<th>percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ItW Boot</td>
<td>75.0%</td>
<td>Standard</td>
<td>77.4%</td>
</tr>
<tr>
<td>ItW File</td>
<td>98.2%</td>
<td>Polymorphic</td>
<td>77.2%</td>
</tr>
<tr>
<td>ItW Overall</td>
<td>88.4%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*LANDesk Virus Protect* shuns the conventional interface, and opts for something different. Unfortunately, in this case it doesn’t entirely work. When the user starts the application, he is presented with a status display detailing the progress of the various scan types. Above this display is a button bar with icons to control various aspects of the product. The icons are misleading and somewhat confusing: in the end, it proved to be easier to use the menus.

When performing an on-demand scan, the user is required to use a frustrating series of dialogs and directory selectors to choose the area he wishes to scan (it is not possible to save these settings). To make matters trickier still, the directory selection window contains important components which are invisible in certain colour configurations – the test server is set up to use the colour scheme ‘Black Leather Jacket’. It took some time to discover what to do with this almost entirely blank dialog box…

The scheduler uses the built-in *NT* schedule service (it even remembers to start the service and set it to automatic start if this has not already been done – a nice touch) to allow scans when no one is logged on, and to allow scans not to be affected by the currently logged on user. Selection of areas is flexible, but has the same problems as the on-demand selection dialogs described above.

The product offers a powerful notification component, with, amongst others, standard message boxes, paging, email, and very configurable SNMP. The notification configuration, however, is shared between all the different scan types.

A real-time scanning component, which is configured from within the main interface, is also included. The choices to be made are whether or not to scan either incoming or outgoing files (or both), which extensions to check, and what is to happen when a virus is detected. Sensible defaults are, of course, provided.

No problems were encountered during the stress testing, but, in common with the *Cheyenne* product, *Intel* could not check files which were loaded from a *NetWare* drive mounted on the *NT* server.

**The BPB Problem**

Every diskette contains, in the boot sector, a table of data which describes its layout – the table is called the BIOS Parameter Block, or BPB. The operating system uses this information to work out how to retrieve data from a diskette.

When a boot sector virus infects a diskette, it needs to write a new boot sector containing its code (or, in most cases, a loader for the rest of its code, stored elsewhere on the disk). It can do this by loading in the current boot sector and overwriting the in-memory image before writing it back, or it can construct an entirely new boot sector in memory, which it can then write out.

In the course of creating the new sector, the virus may need to create a new BPB. If it does this incorrectly, the infected diskette will not be readable by operating systems, which will notice the incorrect BPB and complain. However, the disk will still be infectious; the BIOS is still able to load the boot sector at power on and execute it.

Older viruses make this mistake – they either do not know about, or did not bother to take into account, various disk formats, and some do not simply refuse to infect media they do not understand, but infect with an invalid BPB.
In terms of speed, LANDesk is towards the low end of those products tested – a statement which holds equally true for its detection results. Things really hit rock bottom, however, with the simply staggering 21 false positives! Dearie me.

**McAfee NetShield (v2.5.1)**

<table>
<thead>
<tr>
<th>IW Boot</th>
<th>100.0%</th>
<th>Standard</th>
<th>91.2%</th>
</tr>
</thead>
<tbody>
<tr>
<td>IW File</td>
<td>97.7%</td>
<td>Polymorphic</td>
<td>67.3%</td>
</tr>
<tr>
<td>IW Overall</td>
<td>98.7%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

McAfee ships two Windows NT anti-virus solutions: VirusScan for NT Workstation, and NetShield for NT Server. As expected, each product only installs on the version of NT for which it is designed. [Recent research reveals the true difference between NT Server and Workstation – two registry entries... Ed.]

The product tested was NetShield: it presents itself as a simple list display underneath the expected menu and button bars. This displays available tasks; double clicking on one of these brings up a window displaying the statistics associated with that task. RHB context-sensitive menus are attached to the tasks, making it easy to start, stop or modify the task. For those who prefer buttons to menus, these options are available from the button bar at the top of the window.

Any of the tasks defined can be scheduled to be started at various times on various days, and repeated after given time intervals. They will be fired even if no one is logged on, as they are controlled by the NetShield services. The only problem encountered with these was that if a scan of a mounted NetWare drive was scheduled, it would trigger but fail to scan anything, regardless of whether anyone was logged on at the time. This is a minor failing, but still significant.

New tasks can be defined by creating a default scan, then modifying its parameters to meet requirements, or by using the Scan Wizard, which guides a novice through the process; it’s nice to have both options for novices and expert users in the same product. All configuration options can also be applied to remote NT servers running NetShield – the user chooses a machine to configure from a selection box on the button bar.

Sophisticated alert functions are built in, managed by the AlertManager service. Numerous methods of notification are supported, including pager, network message, printed log, email, and SNMP.

‘Forwarding’ offers the ability to create a centralised server on which all the alerts for the entire NT domain are sent – very useful for those with large networks.

Real-time protection is managed from the main window: the administrator may configure the resident system to scan in/outbound files, to take a particular action when a virus is found, to decide what to do with log file entries, and which files to exclude. There were no problems in the stress test, and the resident software dealt correctly with NetWare drives.

Non-administrative users are allowed to disable the on-access component – on the face of it, it would seem that this should be a system-wide decision, made only by the administrator. However, when a non-administrative user requested the properties dialog for the on-access component, a message box popped up stating ‘Couldn’t connect to the specified computer on the command line: /NOSPLASH /SERVER “RUPERT”’ [Rupert is a VB test-server. Ed.].

Also, users may delete tasks created by other users, including those with higher privileges.

The only thing missing from this product, apart from better security functionality, is the capability to perform centralised and remote updating of other machines on the network from the central server. In the detection tests, the product performed well, only missing out on 100% In the Wild due to missing samples of some of the macro viruses.
disappointing: 95 and NT each offer opportunities to enhance the interface in some fairly radical ways. However, the consistency is a bonus.

The Toolkit offers the usual drive selection box, accompanied by menu options to configure the scanner and integrity checker.

Curiously, it is necessary to go to the ‘advanced’ dialog on the scan selection screen in order to specify which subdirectory to scan: this is not obvious, and is inconvenient, apart from the fact that selecting a directory is not an advanced setting.

Scheduling functionality is provided by a separate user-level application. The application passes settings to the Dr Solomon’s Schedule service: this allows jobs to trigger whether or not a user is logged on, and without the need for a user-level application to be left running at all times.

The real-time component, WinGuard for NT, permits on-access scanning of files locally on the server and remotely from client machines. It does not distinguish between incoming and outgoing files, but does offer selection of the types of objects to be checked.

WinGuard held up well under the stress tests: it did not appear to leak memory or cause undue problems on the server. It also intercepted file access successfully from NetWare volumes mounted on the server.

A nice feature of WinGuard is its ability to be controlled from a Control Panel applet, as opposed to from a section of the main interface. There is a certain symmetry to this – after all, the Control Panel should be used for exactly this type of thing. In common with other such systems, only administrators may modify the settings.

In speed tests, this product clocks in towards the top end of the speed scale, just breaking the 1MB/s barrier on the clean hard drive of the particular machine used for testing. Detection is also very impressive, with the product missing only the two samples of Positron across all test-sets, meaning that it scored 100% in those all-important In the Wild tests.

**Norman Virus Control (v3.52/2.27)**

<table>
<thead>
<tr>
<th></th>
<th>Boot</th>
<th>File</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>ItW</td>
<td>100.0%</td>
<td>97.5%</td>
<td>98.5%</td>
</tr>
<tr>
<td></td>
<td>Standard</td>
<td>Polymorphic</td>
<td></td>
</tr>
</tbody>
</table>

Much of the functionality of this product has already been described when discussing ESaSS TBAVNT earlier in this review – refer to that section for further details.

The only apparent difference between the two installations (apart from the different product name…) is that NVC installs with a ‘Book on Viruses’ help file: whilst this is informative, it is also very out of date. Virus prevalence figures for 1992, anyone?

Detection figures for Norman Virus Control are slightly better than those for ESaSS ThunderBYTE: the same good score against the Polymorphics, a better result in the Standard test-set, and the same on the In the Wild test-sets.

**S&S Dr Solomon’s AVTK (v7.62)**

<table>
<thead>
<tr>
<th></th>
<th>Boot</th>
<th>File</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>ItW</td>
<td>100.0%</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>Standard</td>
<td>Polymorphic</td>
<td></td>
</tr>
</tbody>
</table>

Dr Solomon’s Anti-Virus Toolkit (AVTK) is well-known for its top-notch detection. They have a well-established graphical user interface, used on their products across the Windows range (3.1, 95, and NT). This in itself is fairly
**Sophos SWEEP (v2.87)**

<table>
<thead>
<tr>
<th>IW Boot</th>
<th>81.3%</th>
<th>Standard</th>
<th>99.2%</th>
</tr>
</thead>
<tbody>
<tr>
<td>IW File</td>
<td>100.0%</td>
<td>Polymorphic</td>
<td>93.7%</td>
</tr>
<tr>
<td>IW Overall</td>
<td>92.1%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SWEEP for Windows NT presents itself as an area selection window beneath the menu and button bars. Lit icons represent the areas chosen for scanning, and simply pressing the ‘Go’ icon starts the scan of those areas. A progress bar indicates how the current task is getting on, and a text display at the bottom contains messages.

Cleverly, everything beneath the button bar is actually a property page – the first for immediate (on-demand) scans, the second for scheduled scans. Switching between views allows a user to configure and execute either type of scan, and the application is nicely multi-threaded to allow, say, configuration of scheduled scans whilst an immediate scan is in progress.

Configuration is easy and intuitive, although some scan option pages are curiously designed. Scheduled scans may be configured to run on any combination of the days of the week, and at any number of times on those days. There are other scheduled scan configurations which are specific to particular jobs, and this allows different scheduled jobs to have different configurations.

If one scheduled job fires when another is still in progress, the new job is held until the one currently executing has finished, but an immediate scan can, of course, run concurrently with a scheduled one.

Scheduling is managed by the SWEEP service, which can be configured to log on as a given user to allow network resources to be scanned – the default is to log on as system, in which case network scheduled scans are not possible.

There is no functionality covering the administration of multiple computers, and no on-access scanner as yet. In terms of the interface, support for context-sensitive RHB menu support would be welcome, and more expected as Windows NT moves towards the Windows 95 interface.

The product is among the slower of those tested, and hits the BPB [see panel p.12] problem on scanning diskettes. This aside, SWEEP had no other problems with the In the Wild test-set, and Standard and Polymorphic scores are also very good.

**Stiller Research Integrity Master (v3.02a)**

<table>
<thead>
<tr>
<th>IW Boot</th>
<th>0.0%</th>
<th>Standard</th>
<th>98.0%</th>
</tr>
</thead>
<tbody>
<tr>
<td>IW File</td>
<td>97.3%</td>
<td>Polymorphic</td>
<td>44.5%</td>
</tr>
<tr>
<td>IW Overall</td>
<td>56.1%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This is an intriguing submission for the Windows NT comparative, in that it’s not actually a native Windows NT product, but one for DOS. However, as usual, we did not state that submitted products had to be native NT solutions, and we take what we get.

Integrity Master has a DOS character-mode user interface, which is described and illustrated more fully in this month’s standalone review on p.21. Whilst it is usable and functional, it’s not really quite what a Windows NT user is looking for…

As expected, the product does not offer built-in scheduling, but as it can be driven from the command-line, it is possible to schedule scans using the NT scheduler. Of course, NT-specific features are absent.

One significant problem is that the product cannot check boot sectors from within the Windows NT environment: NT does not allow the appropriate level of disk access, so the product does not try. This is much more elegant than having the NT error box pop up. When used under DOS, the product does detect 74 of the 80 boot sector viruses; however, the problems under NT are rather serious in this regard, and as far as could be ascertained cannot be avoided without the presence of some NT-specific component.

Despite the very reasonable detection in other areas (though the Polymorphic set was a low point), it’s difficult to recommend such a product for use in an NT environment any more – after all, NT has been around for over two years now; it’s time to ask for more.

**Symantec Norton AntiVirus (26/07/96)**

<table>
<thead>
<tr>
<th>IW Boot</th>
<th>100.0%</th>
<th>Standard</th>
<th>87.4%</th>
</tr>
</thead>
<tbody>
<tr>
<td>IW File</td>
<td>98.6%</td>
<td>Polymorphic</td>
<td>56.8%</td>
</tr>
<tr>
<td>IW Overall</td>
<td>99.2%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Norton AntiVirus for Windows NT is available for free download from the Symantec Internet site; be prepared for a long wait, however: it’s a 1.9MB self-extracting executable. Once unpacked, a standard setup program installs the software without problems. It is keen to perform some form of on-line registration; fortunately, however, it is possible to skip this process.
false positive suffered is a definite minus. Sets would set this work off nicely. Unfortunately, the one more work on the detection of other viruses in the other test-sets, this time missing out only on one sample of Desperado.1403.C and all of those of Nuclear.B. A little inch towards 100% detection against the In the Wild positive in this test.

The scheduler is decidedly basic – it only offers the ability to scan all the hard drives at a certain time on one day a week. On the plus side, however, as it is executed by the system scheduler, jobs are fired even when no-one is logged on.

For some reason, the scanning speed, whilst only average on the floppy disk tests, was the fastest of the group on the clean hard drive test; unfortunately, it encountered one false positive in this test.

As far as detection is concerned, the product continues to inch towards 100% detection against the In the Wild test-sets, this time missing out only on one sample of Desperado.1403.C and all of those of Nuclear.B. A little more work on the detection of other viruses in the other test-sets would set this work off nicely. Unfortunately, the one false positive suffered is a definite minus.

Comments

The development cycle of a Windows NT anti-virus product is clear indeed; under normal circumstances, it appears to run like this:

- Stage One: port of Windows 3.1 product, with bolt-on user-level scheduler
- Stage Two: compatibility with NT built-in schedule service
- Stage Three: virus scanning engine installs as a service to permit greater independence from the system and the currently-logged-on user
- Stage Four: real-time scanning file system filter, domain management facilities, centralised updating and reporting

Clearly the exact stages will vary per product, and many products will go through sub-stages on the way, but by and large this is how it works. Every product in this test falls almost exactly into one or other of these categories; the similarities in the development paths are remarkable.

Of the product components, the most technically difficult is the on-access scanner: what is easy under DOS and not overly difficult under Windows and Windows 95 is extremely tricky under Windows NT. On the whole, the four products that include this functionality do it well: Cheyenne and McAfee failed to check files accessed on a mounted NetWare volume, but neither would crash, even under extreme levels of file traffic. McAfee’s system is the easiest and most flexible to control, however.

The domain management features are a slightly different matter: Cheyenne and McAfee approach the same problem from different angles, and consequently reach solutions which appear completely different. Cheyenne’s is probably more powerful at this point, but McAfee’s is far easier to use.

Conclusions

So, when it comes to the crunch, who has the edge? In the opinion of this reviewer, McAfee and Sophos vie for the position of having the most user-friendly interface, but this is an aspect of products in which it is often a matter of preference for each individual user. They are both very easy to use and understand without needing to resort to the manual; McAfee’s, however, has more of the neat little touches that make people sit up and take notice.

Detection rates are a different matter: only AVAST! and Dr Solomon’s AVTK manage 100% on the In the Wild Overall score, and both of these products do extremely well on the other sets as well (AVAST! missed nothing, and the AVTK missed only one sample) – on this basis, the recommendation should be one of these two; however, it seems a shame that neither feels right in the NT environment. They are in many ways inelegant solutions.

The gestation of these products is very much still underway: none is complete at this point in time; right now, I would recommend McAfee as the best all-rounder. If only its detection was a little better, there would be no contest at all.

Technical Details

| Hardware used: | Compaq ProLinea 590, 16MB RAM, 2.1GB disk and a 270MB SyQuest removable drive. |
| Software: | MS Windows NT Server 3.51 with Service Pack Four applied (the current release at the time of product submission). |
| Other technical information: | After reviewing each product, a complete disk image of the OS was restored to the test machine from a sector-level backup on a SyQuest cartridge. Boot sector viruses are all genuine infections, held on 3.5-inch diskettes (one each). The June 1996 WildList (available at http://www.virusbtn.com/WildLists/) was used as the source for the In the Wild test-sets. |
| WWW address for calculation information: | http://www.virusbtn.com/Comparatives/NT/199610/protocol.html |
TEST-SETS

In the Wild Boot Sector Test-set. 80 viruses; each one of:

- 15_Years, AntiCMOS.A, AntiCMOS.B, AntiEXE.A, Boot.437, BootEXE.451, Brasil, Bye. Chance.B, Chinese Fish, Crazy_Boot,
- Parity_Boot.B, Pasta, Peter, QRry, Quandary, Quox.A, Ripper, Russian_Flag, Sampo, Satria.A, She_Has_2, Stealth_Boot.B,

Virus Bulletin OCTOBER 1996 • 17

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.
F-PROT Professional for Windows NT

Martyn Perry

This month a Windows NT product takes a turn under the spotlight; namely, F-PROT Professional for NT v2.23a from the Finland-based Data Fellows.

Licence Considerations

The licence covers the supply of a pre-specified number of base packages which include full documentation. In addition, a pre-specified number of additional manuals and a user’s guide (which may be copied freely) are included.

The licence is granted on a per PC basis which is extended to include the home computers of users based at the office where the licensed software is installed.

Presentation and Installation

The product comes with a single manual with sections for DOS, OS/2, and Windows 3.1, 95 and NT. There are three choices as to the type of installation: Network Administration, Standalone Computer or Update.

For the Network Installation, the user is prompted to select the installation directory for the product (the default is a directory called F-PROTNT underneath the Windows System directory. A shared directory exists for communication between the server and client machines. This is user-defined and must be visible to the users with full (read/write/create/delete) rights.

The installer is prompted for an administrator’s password, and installation will not proceed until one is entered. The files are now copied, with a vertical level meter showing progress of individual files being transferred as well as a normal progress meter for overall installation.

Finally, the installer is prompted to enter his name, and that of his organisation and machine. This creates the F-PROT Professional common program group, which includes the main program as well short-cuts to a number of pre-defined tasks, namely: scan a diskette, scan a hard disk, and scan a network. F-Agent is loaded automatically from the Startup group: it runs in the background to start scheduled tasks, and also takes care of communication between a workstation and the F-PROT administrator.

The application is started with a default task to scan all hard disks when the machine is idle and to report if a virus is found. The default initial configuration does not include the administration facility; however, this can be accessed from the File menu.

Administration

Scanner administration is performed by the administrator logging in to the application by using the password chosen on installation. Administration revolves around managing tasks and preferences – a task is a pre-defined scan; the preferences determine how F-PROT operates.

Preferences cover various areas of the product such as file extensions to be scanned, and how reports are to be handled. A task can be executed either by scheduling it or by running it interactively. A task can be stopped at any time by clicking the Stop button in the dialog window. The program prompts for confirmation: if this is given, it will halt the scan and produce a summary of the incomplete results.

Tasks are defined from the Tasks Menu. Existing tasks can be modified by double-clicking on the task from the task list in the main window, which brings up the ‘Task Settings’ window shown below. Each task is given a name for identification; and for each, several options are available:

- method of scanning used (limited at the moment to Secure only)
- action to be taken when a virus is detected
- drive selection
- selection with browse facility down to individual directories or files

Further settings include a choice of Executables Only or All Files. ‘Executables Only’ scans executable files with default extensions COM, EXE, SYS, OV?, APP, PGM, and BIN. [Interestingly, this does not include DOT and DOC, though these files were checked. Ed.] These can be modified using the Set Preferences options under Scanning. The final option controls the checking of boot sectors on hard and floppy disks.

F-PROT for Windows NT allows the user considerable flexibility in configuring individual scan settings and times.
The type of malware to be detected can also be chosen. This includes Viruses and Trojan Horses and/or, as a separate selection, Document Macro Viruses (the default is both). If both are deselected, the OK button is greyed out, preventing execution of scanning for nothing. A separate section defines what objects will be scanned.

F-PROT has two modes of scanner operation: Immediate and Scheduled. The configuration options for these scans can be pre-defined and stored as tasks. An immediate scan will check the server on demand, using the current immediate settings defined as a task. A scheduled scan allows checks on a defined, timed basis.

To start an immediate scan, set up the task so it is displayed on the task list. Select the specific task required and click start on the task bar. If a virus is found, when the scanner is set to delete infected objects, this message is displayed: ‘The file <filename> is infected. Overwrite and delete the file: Yes, or Yes to All’. The slide bar on scan display can be selected as the scan proceeds, which allows the user to scroll back up to view the messages that have gone off the top of the screen.

In addition to simply scanning at a given time, the scheduled scanning option offers periodic scanning, which can be set to execute at regular intervals after a pre-defined amount of idle time. If Scheduling is enabled, a task can be configured to start only after a defined number of idle minutes.

The date and time choices are comprehensive, allowing scans to be selected, daily, every second to ninth day, on specific days, or a specific day in the month. If specific days are selected, the Week selection can be every week, or second to fourth week. Month selection can be specific month(s), every month, or every second, third or fourth month.

One fairly serious problem with scheduling using F-Agent is that scheduled jobs only trigger when someone is logged on. If this is not the case, the next time the user does log on, they are warned that jobs were missed, and given the opportunity to execute them there and then.

Using F-Agent may thus be a problem on machines used as servers: under normal circumstances no one should be logged on at these machines’ consoles. A more effective strategy, if more complicated to implement, would be to use the built-in NT scheduler, which deals a little [but not much! Ed.] better with not having someone logged on at the time of an event, or to use a service element – services are components of Windows NT which are always running, even when no one is logged on, and under normal circumstances run at a higher level of user privileges than standard user programs.

Configuration Options

The configuration options are referred to as Task Settings. These settings can be created either by copying an existing task and editing its parameters, or by creating a completely new task. Various selections can be made for each task. These include:

- options to scan – this can include local and network drives. This can be extended down to specified directory or file. If the option is left empty, F-PROT will prompt for the directory or file when the task is started.
- objects to be included in the scan: these can be executable or all files and boot sectors
- actions to be taken on virus detection: report only, attempt disinfection, and delete or rename infected file

Reports, Activity Logs, and Communications

F-PROT records executed tasks in the file F-PROTW.LOG. Each entry consists of the task name, execution time and result status. A separate log file reports the results from the task with details of the scan and any viruses detected.

The product supports communication between administrator and users in the form of Bulletins and Messages. These are files which are handled using directories or the server, which is a directory defined with the administrator preferences. The files are created using a separate editor.

Further communication options include having a workstation inform the administrator in the event of a virus being detected, with reports also being sent to the REPORT directory.

In addition, infected and suspect files will be transferred to INFECT and SUSPECT directories respectively, along with the supporting information file. The latter is a useful feature not often seen; it will be helpful for the busy administrator to have the information telling him where this file originated when he has to deal with it.

Tasks can be created by the administrator and distributed to users via the network. F-PROT on local workstations will automatically add any distributed tasks to their local task lists.

Updates

Updates can be distributed over the network using an administrator option. Using this option will copy everything under the administrator’s F-PROT root directory to the
shared UPDATE directory. From there, they are detected by the various clients as they log on, and then copied to their local drives.

The update bulletins are worth a particular mention: they are in newsletter format, and cover changes to the product and new viruses detected. Additionally, news items and details of how the viruses known to F-PROT work are included.

Detection Rates

The scanner was checked using four test-sets: In the Wild, Boot Sector, Standard and Polymorphic — see summary for details. Undetected viruses in the file test-sets were identified using the delete files option and listing the files left behind in the virus directories.

The tests were conducted using the default scanner file extensions supplied. The results were generally good. The In the Wild test produced a 100% result; however, the Standard test only produced 83% success, and the Polymorphic, only 55%. In the Boot Sector set, F-PROT suffered from the common problem of being unable to detect viruses on disks not readable by NT — readers should refer to the Windows NT comparative review for further information. This problem knocked its score against the test-set to 82.5%.

Real-time Scanning Overhead

To determine the impact of the scanner on the server, 50 files making up 6,797,522 bytes (EXE and COM files) were copied from one server directory to another using COPY. The directories used for the source and target were excluded from the virus scan to avoid the risk of a file being scanned while waiting to be copied. The default system setting of Best Foreground Application Response Time was used.

Because of the different processes which occur within the server, the time tests were run ten times for each setting and an average taken. The four tests were:

- Program not loaded. This establishes the baseline time for copying the files on the server.
- Program unloaded. This is run after the other tests to check how well the server returns to its former state. The result in this section is actually fractionally lower than the first, but the discrepancy is well within error.
- Program loaded, but the immediate scanner not running. This tests the impact of the application in a quiescent state, just running F-Agent program which handles the scheduling and communication activities.
- Program loaded and the immediate scan running. This is the full impact of running the scanner on the server files. See the summary for the detailed results.

As F-PROT performs a clean unload of all the files which were originally installed, there is effectively no residual overhead. The effect of the scheduling agent is fairly low, though higher than expected, and the overhead only becomes significant when the scan is running. The impact of this can be adjusted by changing foreground/background response under NT.

Conclusion

The documentation includes a discussion of the impact of viruses with the various operating systems and the clean up processes. The on-line help is available and is a good adjunct to the manual.

The product installs easily, and a deinstall option is included. The product has a good range of options for scanning and dealing with viruses, as well as for communicating between administrator and workstation. One of the few things missing is on-access scanning, which is sure to be on the way.

<table>
<thead>
<tr>
<th>F-PROT Professional for NT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Detection Results</strong></td>
</tr>
<tr>
<td>Test-set</td>
</tr>
<tr>
<td>In the Wild</td>
</tr>
<tr>
<td>Boot Sector</td>
</tr>
<tr>
<td>Standard</td>
</tr>
<tr>
<td>Polymorphic</td>
</tr>
</tbody>
</table>

| **Overhead of On-access Scanning:** |
| Tests show time taken to copy 50 COM and EXE files (6.8MB). Each is performed ten times, and an average is taken. |
| Time | Overhead |
| Not loaded | 7.54 | - |
| Unloaded | 7.52 | -0.27% |
| Loaded, no manual scan | 8.56 | 13.53% |
| Loaded, manual scan | 13.06 | 73.21% |

Technical Details

**Product:** F-PROT Professional for NT, v2.23a

**Developer/Vendor:** DataFellows Ltd, Päiväntaite 8, FIN-02210 Espoo, Finland. Tel +358 0 478 444, fax +358 0 478 44599, WWW http://www.datafellows.com/.

**Distributor UK:** Portcullis Computer Security Ltd, The Grange Barn, Pike’s End, Pinner, Middlesex, England HA5 2EX. Tel +44 181 868 0098, fax +44 181 868 0017.

**Price:** Toolkit base product per year — £180 with monthly upgrades; £140 with quarterly updates. Separate user licence required: 11–50 users, £35/PC (monthly updates), £25/PC (quarterly updates); 51–100 users, £25/PC (monthly updates), £20/PC (quarterly updates). Other prices on request.

**Hardware used:**
Server: Compaq Prolinea 590, with 16MB Ram and 2GB hard disk, running under Windows NT Server 3.51.
Workstation: Compaq 386/20e, with 4MB Ram and a 207MB hard disk, running under DOS 6.22 and Windows 3.1.

**Test-sets:** In the Wild and Polymorphic — see this issue p.17. Standard — see VB July 1996, p.22.
PRODUCT REVIEW 2

A Product with Integrity
Dr Keith Jackson

**Integrity Master** is a software package which describes itself as ‘the fastest, most powerful data integrity and anti-virus software available for any price’ – a sweeping claim. Although the product itself a DOS program, it claims to execute happily under *Windows 3.x*, *Windows 95*, OS/2, and also across networks. This review discusses its abilities under *Windows 3.x*.

**Function**

**Integrity Master (IM)** claims to detect and remove known or unknown viruses, detect file corruption due to hardware or software problems, verify that restored files are intact, and detect file damage. These elements can all be monitored by checking their integrity: the product creates ‘signature data’ (checksums), and verifies that they remain unchanged.

The product can also verify integrity of the boot and/or partition sector, CMOS memory, normal memory, and interrupts. Although the product’s main aim is to check integrity, the documentation states that IM has extensive information about individual viruses – I will return to this.

**Documentation**

The documentation is a single manual (A5, 144 pages long) entitled *Defeating Viruses and Other Threats to Data Integrity*. It is two manuals in one – a User’s Guide, and a section called *Data Integrity and Viruses*. The documentation, refreshingly, advises users not to bother reading all the User’s Guide; but to get on with using the product and resort to on-line help if they get stuck. Would that other products were so candid!

**Installation**

IM was provided for review on one 1.44 MB 3.5-inch floppy disk. Installation proved straightforward, if somewhat tedious. The product installs itself into a subdirectory called IM_HOME. The drive on which IM is installed may be changed, but this subdirectory must have a fixed name, and must be present in the root subdirectory (hence the backslash).

When installation begins, IM asks if this is a ‘brand new install’. Answering in the affirmative, I was then presented with an agreement including the memorable phrase: ‘By accepting this agreement, you agree not to sue us, should you have a problem’.

If the user does not accept this, IM will not install. If the reply is affirmative, the user is asked more questions on performing installation and to state which disks should be ignored, offered a product tutorial, and asked to choose between ‘Fast’ (1 minute) and ‘Full’ (15 to 30 minutes) installation. I chose ‘Full’, mainly as I was not sure of the difference between the two.

Then came two unexpected questions; first: ‘How familiar are you with DOS’? Then I was asked to choose a ‘Security Level’ (Absolute, Very High, Typical, Not Vital). Digging around in the documentation, I discovered that the choices referred to where IM’s checksums were stored; e.g. Very High uses a hidden file stored on a floppy disk. I chose ‘Typical’.

On with the questions. Why am I using IM? (Virus protection, or protection against ‘other’ types of problems?) Err, don’t know – perhaps both would be nice? Do I want speed or convenience? Both, but that is not an explicit option. Would I like ‘Standard File Extensions’? Sounds good. Do I want to check only programs? Perhaps. Whoever installs the product is unlikely to know the answers to such questions.

Installation continues, but not before producing page after page of onscreen instructions as to what I should do. The developers should look at all this: if I purchase a single copy, I will probably not know the answers to many of the questions, and I will guess. If I am a corporate user, I’m going to be fed up at providing these answers over and over again. Either way, it’s pointless.

IM let me choose where to store its integrity files (remember the ‘Security Level’ question?) – the options are either to leave a hidden file in every subdirectory, or to store the
checksums on a diskette. The former scatters files across the hard disk, which I abhor, and the latter requires the user to remember to supply this floppy every time IM is executed.

The floppy disk option is rightly claimed to be more secure (it is more difficult for malware to manipulate the checksums); however, in practice it may well be difficult to achieve. For instance, in many work environments, the user does not set up his own PC, but will have to maintain control of IM’s floppy disk checksum store. I would suggest that IM needs an option to store its checksums within its own subdirectory.

Checking

IM contains many options allowing integrity checking to be tailored in almost any way. A check can be performed on the integrity of an entire disk, on just the files on a disk, on CMOS memory, on the current subdirectory (with or without daughter subdirectories), on specific files, and on the boot or partition sector. IM can reload the boot sector, partition sector and/or CMOS memory from a floppy disk backup if they have been corrupted.

On installation, the product created enough information within its checksum files to permit any of the above integrity tests to be carried out. It even complains about its own files being altered (including its report file!). Surely the developers should take account of this? An option to check only for known viruses (aka ‘scanning’) is included.

Although IM was happy to access the virus test-sets stored on a magneto-optical disk, it refused to check all files on the disk unless it had previously ‘initialised’ the disk; it wanted to create checksum files in every subdirectory of the magneto-optical disk that contained my test-set. No way! The only alternative I could come up with was to copy the test-set onto the hard drive of my test PC (bit by bit, as it is too big for the disk.

[The manufacturers point out that all that is required to prevent the attempted creation of the checksum files is to select ‘integrity Checking: Offer’ and ‘integrity Update: Never’ on the options menu. The MO disk could then be scanned without problems. Ed.]

Checking Speed

When IM was used to check the integrity of my test PC, it was difficult to come up with a measure of how fast it could operate. When used on the entire disk, it checked the hard disk of my test PC in 2 minutes 3 seconds, dropping to 1 minute 55 seconds when only the files on the disk were checked, and plummeting to 3 seconds when only the partition sector and boot sector were checked.

Checking of CMOS memory was (unsurprisingly) virtually instantaneous. IM could search the hard disk for known viruses (i.e. acting as scanner) in 1 minute 58 seconds, rising to 3 minutes 4 seconds when all files were scanned.

Scanner execution time probably provides the nearest thing to a fair comparison as far as IM’s execution timings are concerned. Dr Solomon’s Anti-Virus Toolkit scanned the hard disk of my test PC in 4 minutes 5 seconds. Sophos’ SWEEP in 6 minutes 47 seconds. Both figures were approximately doubled when all files on the hard disk were scanned.

The above measurements show clearly that IM is very fast when used to check the integrity of a disk, and faster at scanning a disk than other market-leading scanners. The two other scanners quoted above are by no means slow, and IM scans a hard disk much faster than either.

Windows Execution

All above timings were measured using IM under DOS. I would like to have provided similar timings for execution under Windows – this proved problematic.

Although the documentation stated that the product runs happily under Windows 3.1, whenever I tried this, IM said it could not find its data files; in particular, MEMW.SRL. No amount of experimentation could change this. Eventually I found a Windows executable file called IMWIN, undocu-mented in the manual – this was my salvation.

When IMWIN was executed, it asked me: ‘Would you like to create the Master Group?’ After an affirmative answer, the product created eleven icons in a Windows group. These were mainly various ways of executing the DOS version of IM to carry out specific tasks, along with help files made available using Notepad.

The product still complained it couldn’t find MEMW.SRL; however, it did now offer to construct the file. Once this was completed, IM could be used in the same way as under DOS. All the timings listed above were roughly 7% slower under Windows, an overhead introduced by Windows itself.

Infuriatingly, IM kept complaining that the integrity of the Windows INI files was altered. Many of these change automatically – exactly how one uses Windows without altering such files is beyond me. I’m sure that with its many options, IM can be set up to ignore such files. The default setting does not do this, though it is obviously possible for IM to detect that Windows is active.
Virus Detection

IM can be used to scan only a disk: as reported, this test executes very quickly, but how good is it at detecting the presence of viruses? I tested this using the test-set referred to in the Technical Details section below.

When IM scanned the viruses in the In the Wild test-set, it stated that 276 of the 286 test samples ‘contain signs of a known virus’, a detection rate of 97%. 150 of the detected samples were defined as ‘suspicious’. IM is a bit vague on what it means by this term, though the report file contained an example that a file with an illegal date/time would be regarded as ‘suspicious’. The product flagged 92 files in the Standard test-set as suspicious, and further stated that 260 of the 265 test samples (98%) contained signs of a known virus.

However they are dressed up, the above figures are quite impressive. Not only is IM faster than most scanners (see above), it is as good as, if not better than, most scanners at detecting known viruses.

Its only problem in looking for known viruses was its tendency to ask me a multiple-choice question whenever it came up with a new onscreen message. One option was not to show a particular message again, but I still had to answer several questions during each scan. If there is a way of stopping this, I did not find it. [Stiller informs us that the ‘Halt’ option on the menu will handle this. Ed.] IM also insisted on user confirmation whenever the current screen became full of messages. The only way I found to stop that one during the above tests was to lay my mobile phone on the space bar to provide multiple, continuous, keypresses! [At VB, this is known as running the product in ‘coffee-mug-mode’, as an empty mug propped on the keyboard comes in handy now and then. Ed.]

The Rest

Several add-on programs are included, which allow IM to be executed when desired, and provide a report on PC configuration. The latter is like a cut-down version of the Quarter-deck program Manifest; it presents information returned by the BIOS, and the low-level attributes of the machine, in an intelligible form – and also manages to include a plug for other programs from the developer of IM!

The final add-on program makes a file which contains a ‘small harmless fragment of the Demolition virus’. This is intended to be used to demonstrate how this product will react to the presence of a virus. It would, perhaps, be preferable if IM were to create instead a copy of the EICAR anti-virus test file, a standardized file which was designed for this very purpose.

IM can be executed from the command-line: this is useful for incorporating integrity checking into batch files. Ump- teen command-line switches are provided to permit this to be tailored. Although it sounds good, bear in mind that IM continually asked questions about what decisions should be taken. It is unlikely that ordinary users who execute standard batch files will know the answers to such questions; thus IM must operate in ‘silent’ mode. The fact that preconfigured batch files are supplied does help here.

Conclusions

Integrity Master is very quick, and accurate, at verifying the integrity of a hard disk. It can check at various levels, and careful configuration will allow the user to reap the benefits. Testing memory and/or interrupts fails miserably if (like me) you use a PC in various configurations.

Its myriad options and endless questions are its downfall. I am sure that it is possible to set it up to verify exactly the desired files, to produce no false alarms, and not to ask the user questions he cannot answer. However, I’m also certain that achieving this state of Nirvana will not be trivial: if PCs on a site are not set up in exactly the same way, some technical support person is in for a lot of work.

What use is IM as far as macro viruses are concerned? These reside in word processor documents which by their nature change continually. To be of help here, integrity checking would need to operate on only those parts of the dormant file that can contain viruses.

I like this product, with its focus on integrity checking, and its inclusion of eminently reasonable scanning facilities. As usual, the legal conditions are both problematical and seemingly over the top; however, they are not vastly different from those of so many other products, and at least the wording (especially in the section about agreeing not to sue) is far clearer than most such products.

Interestingly, IM is the exact inverse of IBM’s anti-virus product. IM is an integrity checker with a scanner thrown in for good measure. IBM provides a scanner with an integral integrity checker. Is the end result really any different?

---

Technical Details

Product: Integrity Master v3.02a, serial no VBVB0132.
Developer: Stiller Research, 1265 Big Valley Dr, Colorado Springs, CO 80919-1014, USA. Tel +1 719 533 1879, fax +1 719 533 1728, email 74777.3004@compuserve.com.
Availability: PC with 310 KB of available memory, running under DOS v2 or above. Also operates under Windows 3.x, 95, and NT, and OS/2. Supports a maximum of 2621 files in a single subdirectory, and warns about using DOS commands APPEND, SUBST or ASSIGN in conjunction with the product.
Hardware used: Toshiba 3100SX: 16 MHz 386 laptop with 3.5-inch (1.4 MB) floppy drive, 40 MB hard disk and 5 MB of RAM, running under MS-DOS v5.00 and Windows v3.1.
Test Viruses: Where more than one variant is used, the number of samples is shown in brackets after the virus name (if the total is greater than one). For a complete explanation of each virus, and nomenclature used, please refer to the list of PC viruses published regularly in VB. For a listing of the boot sector viruses see VB, March 1996, p.23; for the others, see January 1996, p.20.
McAfee has announced a new promotion for anti-virus software users: large corporate users upgrading from a competing product to one of the McAfee products will be offered a discount of 25%. To be eligible, a company must have at least 100 users. A McAfee spokesman commented that this was a ‘great opportunity for users to upgrade to the leading solution that holds a 68% share of the anti-virus sector at a very competitive price’. At the same time, the company has launched NT-ssential, a management suite for NT servers combining anti-virus and backup. The new product integrates NetShield with Seagate’s Backup Exec NT. Details are available from the company; call Caroline Kuipers on Tel +44 1344 304730; email caroline_kuipers@cc.mcafee.com.

Compsec 96, the 13th world conference on computer security, audit, and control will be held from 23–25 October 1996 at the QEII Conference Centre in London UK. The conference will address the problems inherent in security, and risks and threats to IT systems.

S&S International is presenting Live Virus Workshops at the Hilton National in Milton Keynes, Buckinghamshire, UK on 7/8 October 1996. Details are available from the company: Tel +44 1296 318700, fax +44 1296 318777.

Sophys Plc’s next anti-virus workshops will be on 20/21 November 1996, and 29/30 January, 19/20 March, and 21/22 May 1997 at Sophos’ training suite in Abingdon, UK. The two-day seminar costs £595 + VAT. One single day may be attended at a cost of £325 + VAT (day one: Introduction to Computer Viruses; day two: Advanced Computer Viruses). For further information on this or the Practical NetWare Security Workshop (3 October, 26 November), contact Julia Line; Tel +44 1235 544028, fax +44 1235 599935, or access the company World Wide Web page (http://www.sophys.com/).

Reflex Magnetics has another Live Virus Experience scheduled for 9/10 October 1996. Further information is available from Rae Sutton; Tel +44 171 372 6666, fax +44 171 372 2507.

The Computer Security Institute (CSI) 23rd Annual Computer Security Conference is to be held from 11 to 13 November in Chicago, Illinois, USA. The event will feature a program of over 120 sessions, including presentations on Internet security, access, email, etc. It will also include an exhibition of computer security products – free passes to attend the exhibit available from the CSI. For details on attending , contact Patrice Rapalus of the CSI on Tel +1 415 905 2310; email prapalus@csi.}

International Data Security has announced the launch of courses for network protection: Network Security/Management seminars, and Corporate Anti-Virus courses. The one-day Network Security course will take place at various venues in the UK, and will cost £50 per person. The one-day anti-virus course will cost at £400, and will take place at Novell’s UK headquarters in Bracknell, UK. For details on venues and dates, contact Julie Randall of International Data Security; Tel +44 171 209 2222.

Network Security Management has announced the publication of another book; Computer Evidence: A Forensic Investigations Handbook. Written by erstwhile Virus Bulletin editor Edward Wilding (who now works for Network Security Management), the book is available immediately at a price of £39.00. Topics covered include forensic principles, explains legal technicalities, and gives instructions on data recovery. To order, fax Sweet & Maxwell Ltd on +44 1264 342761.