ISSN 0956-9979 JULY 1998

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

IN THIS ISSUE:

• **NetWorthy?** Eleven *NetWare* server scanners face off in this month's comparative review starting on p.11. A high proportion of VB 100% awards may suggest things are getting better.

• **NAI worthy?** *Dr Solomon's* was. This month's News (p.3) and Editorial (p.2) respectively outline and ponder the proposed purchase of *Dr Solomon's Software* by anti-virus and network management giant *NAI*.

• **Apple worthy:** A new threat to Apple machines – and the first native to PowerMacs – is analysed inside. There is debate within the anti-virus community as to whether this is a virus or a worm. Decide for yourself on p.6.

• **Newsworthy:** A new virus, whose mysterious payload was only fully unravelled just days before this issue went to press, is briefly described on the News pages. If you read nothing else in this issue, please read p.3.

CONTENTS

EDITORIAL

Did the Earth Move for You?

It did on the morning of 9 June for anyone in the anti-virus industry.

Perhaps it should not be surprising that the two largest pieces of news in the anti-virus industry in the last six weeks or so have both involved companies from the earthquake belt of California. Last month we reported on the strategic appropriation of *IBM's* anti-virus customers and the licensing of its Immune System for Cyberspace technology by Santa Monica-based *Symantec*. This month, *Symantec's* northern neighbour (and arch-rival) from Santa Clara, *Network Associates Inc* (*NAI*), went one bolder, with the outright purchase of *Dr Solomon's Software*.

"The recent Symantec/IBM deal may have been the spur…"

What does all this mean for the anti-virus industry and you, its customers?

In many ways, it is unclear what the outcome will be. *NAI* says that shortly after the deal completes, it will start shipping both products to corporate users of either. The cynics might say that is a bonus for *NAI's* current customers and a loss for *Dr Solomon's* users. Another, perhaps more generous, interpretation is that it will allow one group to sample the best virus detection available and the other to familiarize itself with a contemporary user interface. Hmmm – OK, maybe this is fairly cynical too…

Within days of the *Symantec/IBM* announcement, competitors were offering 'abandoned' *IBM* customers free or cheap cross-grades to their products (at least in the corporate market). This makes sense in the highly competitive anti-virus market. *IBM's* customers were characterized as having to change their anti-virus supplier. Limiting the choice to *Symantec's* product, as sanctioned by the *Symantec/IBM* deal, was not particularly desirable to any supplier other than *Symantec*. (In fact, in the North American retail market, *NAI* had been offering free cross-grades from various competing products for several months prior to the *Symantec/IBM* agreement. Given its market share, this effectively forced its main competitors to follow suit.)

The recent *Symantec/IBM* deal may have been the spur for *NAI's* purchase of *Dr Solomon's*. Recently, the core virus detection technology in *NAI's VirusScan* product range has been showing its age. There have been several changes (including the addition, then removal, of 'Hunter technology') and these, coupled with other revisions of various magnitudes, seem to have resulted in some stability problems and increasingly slow performance. Within the industry, various commentators have been suggesting that it was fast approaching time for a major change within *VirusScan*. If *NAI* saw any threat in the *Symantec/IBM* agreement, now would be the time to act.

The complexities of creating a new virus detection engine from scratch, or of significantly re-engineering one to greatly improve performance, are such that, given *NAI's* size and wealth, outright purchase of an existing, better, product would have to be considered a possibility. From this perspective, the proposed purchase of *Dr Solomon's* is perhaps not that surprising.

But why *Dr Solomon's* specifically? The suspicion is that *VirusScan's* market penetration in the UK (and other parts of Europe) is not what *NAI* would like, so purchasing a significant player in that market makes sense – at least so long as *NAI* can retain the brand loyalty. In fact, much of the *NAI*-generated information about the purchase focuses on this aspect of the deal. I guess it is un-American to admit you had to buy foreign technology to drag your product up to scratch!

But where *will* things go? I have talked to some distinctly anti-*NAI* people. The image of the crass, hype-it-for-all-it-is-worth days when John McAfee was at the helm still haunts these people. Adamant they will not buy *McAfee/NAI* products, other vendors will benefit from their custom. Bill Larson, the CEO of *NAI*, made several references to *Microsoft* in a press briefing I attended. He comes over as the Bill Gates of the emerging 'network and desktop management' market that *NAI* claims to be shaping itself for. The days of 'suites' of anti-virus, remote control, network security, personal encryption and 'zero administration' management software, bargain-priced and almost regardless of individual component quality, may be upon us.

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

NEWS

Wise Purchase by NAI?

Network Associates Inc (*NAI*) continues its 'buy your way to success' approach with its acquisition of *Dr Solomon's Software*. The definitive share transfer agreement values *Dr Solomon's* at approximately US$640 million.

Announced on 9 June, the acquisition is expected to be completed within 90 days, subject to *Dr Solomon's* shareholder approval and the deal meeting various regulatory requirements. The directors of *Dr Solomon's* are recommending that the offer be accepted by shareholders.

Formed late last year from the merger of *McAfee Associates* and *Network General*, *NAI* acquired the encryption software developer *Pretty Good Privacy Inc*, late last year. In 1998 *NAI* has also purchased network security specialists *Trusted Information Systems Inc* and help desk management software developers *Magic Solutions International Inc*.

Initial indications are that the next major upgrade of *Dr Solomon's Anti-Virus Toolkit* (*AVTK*) will continue, as planned, this autumn. Once the transaction closes, both product lines will be included in *NAI's* product suites, so corporate customers of either product will have the chance to familiarize themselves with both. Early in 1999, *NAI* expects to begin shipping an upgrade 'incorporating the best of *Network Associates'* and *Dr Solomon's* technology'. This will be free for corporate subscribers to either product.

In the retail market, *NAI* claims it will continue with all three existing products – *NAI's McAfee VirusScan*, and the two *Dr Solomon's* retail products *HomeGuard* and the *AVTK*. When asked how long for, *NAI* CEO Bill Larson immediately answered 'Forever'. It seems that the amount of retail shelf space 'real-estate' you cover is an important factor in that market segment.

Little has been said about Macintosh anti-virus software in the wake of this news, but it should be of interest to Macintosh owners that *NAI* now owns two of the three major products for the Macintosh platform: its own *VirusScan for the Mac* (based in part on the now retired *Disinfectant*; see *VB* June 1998, p.3), and *Virex* which *Dr Solomon's* purchased from *Datawatch Corporation* in October 1997 and that has replaced the Macintosh version of the *AVTK* ▮

News Flash

A virus with a highly damaging, and previously unseen, payload was isolated in the middle of June. Some reports of infections by this family of three PE infectors, which only work under *Windows 9x*, have been received from the field. Further, the payload of two of the variants triggered on 26 June, damaging machines in Asia and Europe.

The virus has been ascribed various names [*as is the norm in this industry – Ed*] but most include 'CIH' from a string in the virus. To the technically oriented, CIH also included an interesting variation on the cavity attack – *VB* hopes to carry a detailed analysis of CIH in the August issue.

Initially, the payload was thought to involve a disk trashing routine. Fourteen sectors at the beginning of head zero on every cylinder of each hard drive are overwritten with random data. This would, at the very least, render the system unbootable and lead to expensive data recovery procedures should the disk contents not be backed up.

However, literally hours before the two variants that triggered on 26 June were due to start wreaking havoc, it was discovered that the payload was potentially much more damaging than was first thought. Richard Wang, a virus analyst at *Sophos*, confirmed that a small part of the code in the virus' payload could corrupt the contents of the Flash ROM of many PCs. The Flash ROM (technically an EEPROM) contains the BIOS and the activation code included in the CIH viruses would work with a large number of Pentium motherboards based on popular *Intel* chipsets. The relative obscurity of this code meant that it had not been understood by others who analysed it.

The possibility of a virus (or Trojan) corrupting Flash BIOSes has been known for several years. Jakub Kaminski, *Virus Bulletin*'s Technical Editor, presented a paper at *VB'95* describing the state of the art of Flash ROM technology and the attendant risks. He concluded that the safest position to adopt was to disable the Vpp programming voltage, rendering the EEPROM unwritable.

It seems many motherboard or PC manufacturers have not fully considered these issues. Many computers nowadays ship with Vpp enabled, leaving your only line of effective defence down. In laptops, little can be done – most are hard-wired to writable mode. Most desktop motherboards however, have jumpers to set the Vpp voltage (usually a choice of 5V and 12V is offered). What is seldom made clear is that not setting either option may effectively disable Vpp, therefore leaving your BIOS 'safe'.

The likelihood of your having contracted this virus is very small. However, given the serious consequences of its payload triggering and the concern that now the technique is known other virus (and Trojan) authors may copy it, you may wish to ensure your PCs' BIOSes cannot be unintentionally 'flashed'. If you are concerned about this, *Virus Bulletin* advises that you clarify with your system supplier the correct method of *disabling* EEPROM Vpp on your motherboard and that you ensure that machines purchased in future are shipped with Vpp disabled. *VB* further advises that, in general, you should avoid purchasing systems that cannot have EEPROM Vpp disabled ▮

IBM PC VIRUSES (UPDATE)

The following is a list of updates and amendments to the *Virus Bulletin Table of Known IBM PC Viruses* as of 15 June 1998. Each entry consists of the virus name, its aliases (if any) and the virus type. This is followed by a short description (if available) and a 24-byte hexadecimal search pattern to detect the presence of the virus with a disk utility or a dedicated scanner which contains a user-updatable pattern library.

Type Codes

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

Ask.352
ER: An encrypted, 352-byte appender. The virus displays the name of a file called for execution and infects it, only if a user presses the 'y' key. Infected files have the word 4D48h ('HM') at offset 0012h.
```
Ask.352          1E06 E800 005B 5383 C317 90BA ???? B9F4 012E 3117 E306 4343 4949 EBF5
```

Bel.2124
CER: A polymorphic, 2124-byte appender (effective virus size) containing the texts '▮ reBEL.P1 ▮ (Belarus).' and 'Hi, Mr. Kolyada!'. This template detects the virus in memory only.
```
Bel.2124         B8FF 54BB 0201 CD21 86FB 3BC3 7502 EB63 1E58 2D04 008E C026
```

Coca.509
CR: An appending, 509-byte virus containing the text 'Coca-Kola 1.0 By Raven'. The payload, which triggers on Sunday after 6pm, displays the message 'System halted.', followed by a message, in Russian, asking a user to pour Coca-Cola in the disk drive in order to cool it down.
```
Coca.509         B2E9 8816 0102 B440 BA00 00B9 FD01 CD21 B800 4233 C933 D2CD
```

Companion.181
PCN: A companion, 181-byte, direct, fast infector containing the text '*.COM'. The virus changes COM extensions to CON and copies itself under the original file name, setting its attribute to hidden.
```
Companion.181    B43C B902 00CD 218B D8B4 40B9 B500 BA00 01CD 21B4 3ECD 21C3
```

Crasher.439
CR: A prepending, 439-byte virus containing the text '(C) CRASHER X'. The 'Are you there?' call Int 21h AX=ACDCh returns the value AX=DADAh.
```
Crasher.439      26C6 060E 00CB B8DC ACCD 213D DADA 7503 EB72 90B8 2135 CD21
```

Crasher.659
CR: A 659-byte prepender containing the texts '(C) CRASHER X' and 'Dear users ! Hapy new year !' with a Christmas tree image. The payload, which triggers after 20 December, overwrites the first 1536 sectors on the C: drive. The 'Are you there?' call Int 21h AX=DDDDh, returns the value AX=DADAh.
```
Crasher.659      26C6 060E 00CB B8DD DDCD 213D DADA 7503 EB7E 90B8 2105 80C4
```

Dikshev.1334
CN: An encrypted, 1334-byte, fast, direct infector.
```
Dikshev.1334     B945 02CC 33C2 CD01 E2F9 8BDD 81C3 BF00 0E33 C08E C0FA 2689
```

Dre.756
CN: An encrypted, appending, 756-byte, fast, direct infector containing the texts '????????COM', '*.COM', 'ZTKNEW.COM', '*.EXE' and 'Wr. by Doctor Dre 1997(c).King V1.2'.
```
Dre.756          C98A 0428 8605 0146 4541 81F9 B602 7403 E9EE FF2B E9E9 70FD
```

Earle.1431
CER: An appending, 1431-byte virus containing the texts 'COMEXE' and 'This program is dedicated to my girlfriend Gabriela, who hates computers. SWITCH v 1.3 (C) by Windom Earle'.
```
Earle.1431       B440 8B1E 9600 B997 0533 D29C 2EFF 1E98 0073 02EB 653B C174
```

Exeheader.337
ER: A 337-byte virus inserting its code in EXE headers. It contains the text '[Serrelinda], Rhince/VLAD'.
```
Exeheader.337    B89C 00BA 1325 92CD 215B 8EDB 8EC3 83C3 102E 011E 8A00 4189
```

Exeheader.352
ER: A 352-byte virus which inserts its code in the unused area of EXE file headers. Infected files have the word 6F53h ('So') at offset 01FDh.
```
Exeheader.352    B960 0133 C0FC F3AE 7556 C607 E98A 4702 2EA2 FC02 C747 019D;
```

Leo.333
EN: A 333-byte virus which inserts its code in the unused area in EXE file headers. It uses the MZ header, but infects only NE files. It contains the encrypted texts '*.exe' and 'This program requires Microsoft Windows.' The first three words of the second message are in Russian.
```
Leo.333          B440 B94D 01BA EDFF 03D7 CD21 B409 B92E 00BE E600 03F7 E816
```

Leo.1965
CEN: A 1965-byte virus containing the encrypted texts 'Version 3.0.', 'Virus has written by Leo..', 'Korolev city 1998' and 'command.com'. The virus also infects NE files with the Leo.333 virus.
```
Leo.1965         B440 B9AD 078B D583 EA13 CD21 B800 4233 C933 D2CD 21B4 40B9
```

Masha.1338
ER: An encrypted, appending, 1338-byte virus containing the text 'I ♥ Masha (c) by S.V. I Love this Name' and another message in Russian, unreadable without the special driver. Infected files have the ASCII string: 'Masha1' at the end of code.
```
Masha.1338       E93D 05B9 1F05 BF13 012E A132 062E 3105 47E2 FA??
```

Nucleii.200 **CN:** An overwriting, 200-byte virus containing the texts '*.*C*', '..*' and 'nUcLeii~.E=mc2'.
```
Nucleii.200          B9C8 00B4 40BA 0001 CD21 595A B801 57CD 21B4 3ECD 21B8 0143
```

Opa.90 **CER:** An overwriting, 90-byte virus containing the text 'JO4'.
```
Opa.90               1E1D 018B D8B4 401E 0E1F BA00 01B9 5A00 9C2E FF1E 1D01 1FCF
```

Opa.200 **CER:** An overwriting, 200-byte virus containing the texts 'COMMAND.COM' and 'JOPA5'.
```
Opa.200              1E03 018B D8B4 401E 0E1F BA00 01B9 C800 9C2E FF1E 0301 1FCF
```

Opa.600 **CER:** A prepending, 600-byte virus containing the text 'JOPA6'.
```
Opa.600              B440 2E8B 1E10 011E 0E1F BA00 01B9 5802 9C2E FF1E 0801 1FB8
```

Pindonga.3551 **CER:** A polymorphic, stealth, encrypted, 3551-byte virus containing the texts 'PINDONGA Virus (Programado por OTTO en ARGENTINA) 16977.', 'ANTI-VIR.DAT', 'PINDONGA Virus V4.3. (Hecho en ARGENTINA)', 'Saludos a MAQ-MARIANO-SERGIO-ERNESTRO-COSTRA-TORDO-PABLIN', 'Programado por OTTO (16977)', 'CHKLIST.MS', 'PD: Alguien mate a Bill Gates (El WINDOWS SE CUELGA)' and 'PINDONGA Virus (Programado por OTTO en ARGENTINA) 16977'. There is no simple template to detect infected files – the following may be used to detect the virus in memory only.
```
Pindonga.3551        B440 B9DF 0D2E FF36 3605 5A02 D632 F601 D133 D2CD 851E 061F
```

Possessed.2167 **CER:** A 2167-byte appender (EXE) and prepender (COM) containing the texts 'POSSESSED! Bwa! ha! ha! ha! ha!' and 'Author: JonJon Gumba of AdU'. Infected EXEs have the word 1970h at offset 0012h.
```
Possessed.2167       B977 08BA 0000 B440 E8AF 0172 DE8B 0E62 008E 1E64 00BA 0000
```

Sergeant.229 **CR:** An appending, 229-byte virus installing itself in the Interrupt Vector Table. Infected files have the word 5354h ('TS') at offset 0003h.
```
Sergeant.229         0500 CD21 E815 00B4 40BA BC02 B9E5 00CD 21B4 3ECD 215A 595B
```

Spanska.1008 **CN:** An encrypted, appending, 1008-byte direct infector containing the texts 'Remember those who died for Madrid No Pasaran! Virus v2 by Spanska 1997', '*.*' and '*.c*'. Infected files have the word: 636Ch ('lc') at offset 0003h.
```
Spanska.1008         C38A 96FE 04B9 B903 8DB6 4001 8BFE 8A04 4632 C2E8 D4FF E2F6
```

Spanska.1509 **CEN:** An encrypted, appending, 1509-byte direct infector containing the texts '*.*', '*.C*', 'Mars Land, by Spanska(coding a virus can be creative)' and '*.E*'. Infected files have the word 6565h ('ee') at offset 0003h (COM) and at offset 0012h (EXE).
```
Spanska.1509         AAC3 8A96 2701 B9B4 058D B640 018B FEAC 9032 C2E8 EAFF E2F7
```

Spooky.440 **CN:** An overwriting, 440-byte virus containing the texts 'C:\windows\command', 'C:\windows\system', '*.c*', '*.*', and 'Which is stronger Man or Chu locked in endless warfare fighting over empty names using up peoples strength Stella, coded by Opic [codebreakers],1998'.
```
Spooky.440           89F7 B989 01E8 0300 E90E 00AC 9032 062E 0190 AA90 E2F5 90C3
```

Vicky.304 **CN:** An overwriting, 304-byte direct infector containing the texts '*.AOM', 'Demon. Version 2.5 , modified by Beholder' and 'I love you , Vicky! Come back! I forgived you !'.
```
Vicky.304            BA00 01B4 40EB 00B9 3001 EB00 CD21 90B8 0157 8B16 C501 EB00
```

Vicky.567 **CR:** An appending, 567-byte virus containing the texts 'I hate Nirvana !' and 'SMYO=MOTBSMS BOTID)V_ 2007 VTSDJRT C'.
```
Vicky.567            B909 00F3 A674 2933 D2B9 4002 B440 CD21 721E B800 4233 D233
```

Vicky.1015 **CER:** An appending, 1015-byte virus containing the texts 'I love Vicky', 'EXECOM' and 'Life is shit,love is all!'. Infected files have the string 'VTSDJRT▌C' at the end of code.
```
Vicky.1015           B9F7 03B4 40E8 3CFE C3B8 0242 33D2 8BCA E831 FEC3 B800 4233
```

Vicky.1109 **CER:** An appending, 1109-byte virus containing the texts 'I love Vicky', 'EXECOMLIFE' and 'Life is shit,love is all!'. Infected files have the string 'VTSDJRT▌C' at the end of code.
```
Vicky.1109           B955 04B4 40E8 3CFE C3B8 0242 33D2 8BCA E831 FEC3 B800 4233
```

Vicky.1186 **CN:** An overwriting, 1186-byte direct infector containing the texts '*.COM', 'Demon. Version 2.0 , modified by Beholder' and 'Love is all...When you falling love ,life seems like a dream.Wonderfull dream !But when she leaves you.. Why don't you come back to me, my dear? I need you,I want you ,I love you , I already forgived you !'.
```
Vicky.1186           BA00 01B4 40EB 00B9 A204 CD21 90B8 0157 8B16 AF01 EB00 8B0E
```

Yusong.1471 **CER:** An appending, 1471-byte virus containing the texts 'ERROR IN EXE FILE' and 'This program is only a test.It does nothing to you. You are lucky to meet me.Thank you very much. Bye bye ! (C) Copy right by Yusong,3,1997. All right reserved !'.
```
Yusong.1471          B9BF 06BA 0001 2BCA B440 9CFF 1E0C 01E8 72FF C38B 1E14 01B8
```

Zlodic.666 **CN:** A 666-byte direct infector infecting one file at a time. It contains the texts 'Kolya lives .. somewhere in Moscow', '-=SPARTAK(MOSCOW) - CHAMPION FOREVER!=-', 'ANARCHY', 'VIVAT EGOR LETOV. PUNKS NOT DEAD', '*Zlodic.666*' and '*.C*m'. Infected files have the byte 90h at offset 0004h.
```
Zlodic.666           B440 8D96 0601 3E8B 8E9E 03CD 66B8 0042 33C9 33D2 CD66 B440
```

Prevalence Table – May 1998

Virus	Type	Incidents	Reports
Cap	Macro	74	18.5%
Mental	Macro	22	5.5%
AntiExe	Boot	21	5.3%
AntiCMOS	Boot	20	5.0%
Form	Boot	20	5.0%
Parity_Boot	Boot	18	4.5%
Laroux	Macro	17	4.3%
Ripper	Boot	17	4.3%
Concept	Macro	14	3.5%
Dodgy	Boot	10	2.5%
DelCMOS	Boot	9	2.3%
Wazzu	Macro	9	2.3%
Empire_Monkey	Boot	8	2.0%
NYB	Boot	7	1.8%
Quandary	Boot	6	1.5%
Sampo	Boot	6	1.5%
ABCD	Boot	5	1.3%
Junkie	Multi-partite	5	1.3%
Appder	Macro	4	1.0%
Autostart.9805	File	4	1.0%
Npad	Macro	4	1.0%
Tequila.2468	Multi-partite	4	1.0%
Baboon	Boot	3	0.8%
Esperanto.4733	File	3	0.8%
MDMA	Macro	3	0.8%
Moloch	Boot	3	0.8%
Muck	Macro	3	0.8%
WelcomB	Boot	3	0.8%
Others [1]		77	19.3%
Total		399	100%

[1] The Prevalence Table includes two reports each of: ABC, Angelina, Counter, Eco, Hare.7610, Imposter, Johnny, LBB_Stealth, Natas, Razer, Schumann, Spirit, V-Sign and WereWolf; and one report each of: Allen, Beryllium, Bravo, Cascade, Casper, CopyCap, CSV.5536, Diablo, Diskboomer, DZT, Exebug, Extras, Galicia, Gest, Goldfish, Hark, INT-CE.2560, Jerusalem.1363, Keypress.1215, Killer.2352, Komcon, Lunch, Macaroni, MacGyver.4643, Minimal, NF, One_Half, Overboot, Pirates_Hat.2360, Rapi, RDA_Fighter, Rehenes, RP, RPS, ShowOff, SMEG.Pathogen, Spanish_Telecom, Spanska.4250, Stealth_Boot, Swlabs, Tai-Pan.438, Timid.263, Trout-7884, Twno, Urkel, USTC.7680, Virogen.Pinworm, Wallpaper and Win95/Lizard.

Readers are reminded that more detailed listings are posted at http://www.virusbtn.com/Prevalence/.

VIRUS ANALYSIS

Worms in the Ripe Apple

Craig Jackson
Dr Solomon's Software, USA

While the numbers of PC-specific and cross-platform macro viruses have grown dramatically over the past four years, the number of Macintosh-specific viruses has remained unchanged. That is, until recently.

In May this year, a new Macintosh worm was discovered – AutoStart 9805-A. A worm is a class of virus that replicates but does not attach itself to other pieces of code. [*This is a point of some contention. Ed*] The worm was originally reported by a desktop publishing firm in Hong Kong. It had a number of infected clients experiencing strange disk activity on their Macintoshes.

Similar reports were soon to follow from a variety of businesses in the new Chinese province. Within a month of its discovery, AutoStart 9805 surfaced elsewhere in the world, with incidents in mainland China, Taiwan, the Philippines, Australia, Japan, New Zealand, the United Kingdom, Canada, and several sites in the United States.

Three more AutoStart 9805 variants were identified in the following weeks. All of these appear to be written by the individual responsible for the original variant. Hints of an evolving conscience may be seen in the first – AutoStart 9805-B removes AutoStart 9805-A when infecting and will cease to operate after 24 December 1998. The later two variants take this a step further, scanning for and removing all known variants before removing themselves. AutoStart 9805-C self-destructs after 8 June 1998. AutoStart 9805-D is functionally equivalent to the -C variant, except that it self-destructs after 24 December 1998.

While the damage is done, with four new viruses now in the wild and a concept introduced to would-be imitators, it is to be hoped the strange way of 'apologizing' marks the virus author's retirement. The AutoStart 9805 viruses are interesting for more than the associated narrative. These are the first viruses designed for the PowerMacintosh platform and, while they fail to operate on earlier Macintosh computers, they are extremely prolific. Their success is due to their unique infection mechanism, based on a minor aspect of *Apple's* QuickTime services: the AutoStart feature.

Infection in QuickTime

QuickTime is *Apple Computers'* series of cross-platform multimedia services. Commonly associated with its digital video component, QuickTime also has applications in music, speech, interactive media, imaging, character animation, and virtual reality. However, some QuickTime services can be readily abused.

QuickTime AutoStart, introduced in QuickTime v2.0, allows a document or application to load automatically when CD-ROMs, or other removable media, are inserted into a QuickTime-enabled machine. AutoStart was intended to make the QuickTime experience more accessible and has been used to simplify the installation and execution procedures for some applications, but little thought was given to its security.

The AutoStart information is stored in the media's boot sector. There is one field per boot sector, which allows one AutoStart process to be registered per volume. The required boot sector field exists only on disks using *Apple's* Hierarchical File System (HFS or HFS+) formats. These formats are used by MacOS and, while QuickTime services are available for a variety of platforms, the AutoStart functionality is supported exclusively on the Macintosh.

The AutoStart 9805 viruses enter the system on removable media. When infected media are inserted in a machine, the virus is loaded by the QuickTime AutoStart mechanism. Once loaded, the virus will copy itself into the Extensions folder on the startup volume, hide its own icon, and return control to the system or, in the case of AutoStart 9805-A, reboot the machine.

When an infected system is restarted, the virus is loaded from the Extensions folder by the Macintosh operating system. Once active, it tests all mounted volumes every few minutes for an infection. If it is satisfied a volume is clean, it copies itself into the root directory of that volume, hides its own icon, and installs itself as the AutoStart process for that medium. Thus the virus replicates.

Power to the Macintosh

The Macintosh computer was designed around the *Motorola* 680*x*0 series microprocessor. This series was quite advanced for its time, with a large register file, architectural support for 32-bit arithmetic, linear addressing, and basic operating system protection. When the Macintosh computer was introduced in 1984, it was assumed that a member of the 680*x*0 series would provide the foundation for the Macintosh platform's lifetime.

After a decade of refinements, the 680*x*0 architecture was all but exhausted. *Motorola* and *Apple* needed a competitive microprocessor to meet the increasingly demanding needs of the personal computer market. Complementing their engineering team with scientists at *IBM*, the consortium began work on the PowerPC.

The PowerPC was based on *IBM's* innovative POWER1 microprocessor. Many times faster than the fastest 680*x*0, its adoption sacrificed binary compatibility, so programs for earlier Macintoshes would not run. *Apple's* solution was to emulate older 680*x*0 code in software. Thus, shortly after the 1993 introduction of the PowerPC 601, *Apple* released the PowerMacintosh based on the new chip which included the ability to execute MC68LC40 code in software.

With the introduction of the PowerMacintosh, there was a need for an executable to contain several machine code representations of a given program: 680*x*0 code for compatibility with earlier Macintoshes and PowerPC native code in the interest of efficiency. Thus, the Code Fragment Manager was introduced.

Every Macintosh file contains two parts: a resource fork, which contains data used by an application, such as menus, dialogs, and icons, and a data fork, which contains data specific to an application. Traditionally, the resource fork contains all application code.

When an application is loaded, the Code Fragment Manager checks the executable's resource fork for a code fragment resource ('cfrg'). If found, the information in this resource is used to determine the location and type of machine code available for execution. In most cases, the PowerPC code will be located in the data fork of the executable, and 680*x*0 code will be located in the resource fork.

There are currently three basic types of MacOS executables. They are 680*x*0 native, PowerPC native, and Fat. 680*x*0 native applications do not contain native PowerPC code, but can be emulated on the PowerMacintosh. PowerPC native applications do not contain any 680*x*0 code, and are incompatible with earlier Macintoshes. Fat applications contain native code for both platforms.

Some older MacOS viruses are unsuccessful on PowerPC-based Macintoshes. While they are written in 680*x*0 code capable of executing inside the PowerMac emulator, the viruses fail to update the code fragment resource in newer executables to make their code active.

Conversely, the AutoStart 9805 viruses are only native to PowerPC – they do not include 680*x*0 code, and will not operate on 680*x*0-based Macintoshes. On 680*x*0 machines, an error dialog will appear and the virus will fail to execute. However, future variants could easily be designed to operate on all Macintoshes.

Developing a Conscience

The four known AutoStart 9805 variants share a common replication mechanism, but the behaviour of each is unique. AutoStart 9805-A resides in a hidden file named 'DB' in the root directory of infected media, and in a file called 'Desktop Print Spooler' in the Extensions folder on infected machines. These files should not be confused with their perfectly legitimate counterparts, 'Desktop Printer Spooler' and 'Desktop DB', found on all recent Macintosh systems.

AutoStart 9805-A replicates onto uninfected media every thirty minutes and then activates its damage routine. The virus will overwrite up to 1 MB of information with garbage data in files with a data fork over 100 bytes in length and the file extension '.DATA', '.COD', or '.CSA'; and in files over 2 MB in length bearing the '.DAT' extension. It is the only variant which forces a restart of the

machine after the initial infection. AutoStart 9805-A is also the only variant that attempts to infect network volumes. QuickTime AutoStart information is not accessible on network volumes, so although the virus is copied, it cannot be made active through the AutoStart mechanism.

The second variant, AutoStart 9805-B, resides in a slightly obscured file named 'BD' on infected media, and 'Desktop Printr Spooler' on infected machines. It infects media every three minutes and triggers every six. When triggering, the virus will overwrite up to 1 MB of data following the first 10 KB in JPEG, TIFF, and Encapsulated Postscript files in up to twenty previously undamaged files.

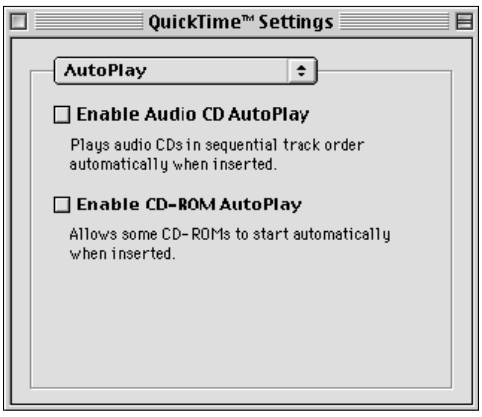
The virus determines a file has already been damaged by ensuring the first byte of the overwritten area is zero. It will only trigger if the 'Extensions:Printer Descriptions' folder does not contain files beginning with 'ACR', 'GEN', 'COL', 'LAS', or 'DIS'. It is suspected this was done to limit the damage routine's impact to specific publishing houses, who are prone to use less common printer configurations. AutoStart 9805-B explicitly removes the earlier AutoStart 9805-A virus when infecting and stops spreading and triggering after 24 December, 1998.

The -C and -D variants seem to be attempts to clean things up. Both remove the -A and -B variants, and reside in the 'DELDB' file on infected media, and the 'DELDesktop Print Spooler' file on infected hosts. The replication mechanism triggers every ten minutes. If executed after 8 June 1998, AutoStart 9805-C attempts to remove itself. AutoStart 9805-D stays active longer, throttling its replication trigger back to a 25 minute interlude after 31 October, finally trying to remove itself after 24 December 1998. In either case, the virus is unsuccessful in removing the active copy of itself and does nothing to prevent reinfection.

Countermeasures

These viruses are only successful on machines supporting QuickTime AutoStart. While it is possible to remove QuickTime extensions from a machine, under QuickTime v2.5 and later it is also possible to disable the AutoStart feature independently.

The QuickTime Settings control panel has the option to Enable CD-ROM AutoPlay in the AutoPlay panel. The name of this setting is slightly misleading, as the option actually enables the AutoStart function for all media. Clearing this checkbox prevents the AutoStart 9805 viruses from infecting the machine. Note, however, that this does not prevent the virus from infecting additional media if the machine is already infected. As always, the recommended solution is to use an anti-virus package with regularly updated virus definitions.



Conclusion

The AutoStart 9805 viruses introduce a new form of infection mechanism and break the silence of Macintosh virus evolution. They are successful and precedent-setting, but they are also easily preventable.

AutoStart 9805

Aliases: Hong Kong Virus.

Type: PowerMacintosh QuickTime AutoStart infector.

Infection: AutoStart media and installs itself as a MacOS Extension.

Self-recognition: The presence on media and in the Extensions folder of appropriately named files. In addition, the -B variant detects the earlier -A variant, and the -C and -D variants both detect the -A and -B variants.

Hex pattern: -A variant

```
7C03 0050 2800 0708 4180 001C
4800 0069 6000 0000 4800 0FAD
```

-B variant

```
801E 0000 3C60 B2A8 3863 244D
7C00 1840 4180 000C 4800 A621
```

-C variant

```
801E 0000 3C60 B1A2 3863 C4B8
7C00 1840 4180 00E8 4800 0241
```

-D variant

```
801D 0000 3C60 B260 3863 F795
7C00 1840 4181 0010 3800 0258
```

Payload: The -A and -B variants overwrite data files with up to 1 MB of garbage.

Trigger: -A variant every 30 minutes, -B variant every 6 minutes, and every 10 minutes for -C and -D variants. -B and -D variants stop infecting after 24 December 1998, and the -C variant stops infecting after 8 June 1998.

Removal: Disable QuickTime AutoStart (see text) then restart while holding down the shift key (to disable extensions). Delete the appropriate files from the Extensions folder and from infected media.

OPINION

Talking Trojan

Ian Whalley
Sophos Plc

Listen to some in the anti-virus industry, and you might well believe that computer viruses are a thing of the past. Trojans, they will tell you, are the way of the future. Indeed, they are so keen to tell you this that you would be forgiven for forgetting entirely about the continuing threat from viruses – the very creations that brought us in the anti-virus industry both a name and a living, and against which we continue to struggle.

Similarly, there are those who will tell you that Trojans are nothing to worry about, and that the other faction is clearly either seriously mistaken or deliberately attempting to mislead. The truth, as is so often the way, lies somewhere between the two extremes. As in modern politics, the path to success is at neither end of the spectrum, it lies somewhere along the centre ground.

Terminology Trauma

As is well known, the word 'Trojan' derives from the wooden horse that the Greeks constructed to gain access to the city of Troy – it was offered as a gift of peace by the apparently retreating Greek army. Unbeknownst to the confused Trojans (they must surely have been confused, or they would not have fallen for such a ruse), inside the horse the equivalent of the Greek Special Forces lay in wait. The horse was dragged inside the city walls, night fell, out climbed the Greeks, and that was the end of Troy. Exactly why the horse is referred to as the Trojan Horse and not the Grecian Horse, mythology does not relate.

In the field of computers, therefore, a 'Trojan Horse' is a program the true purpose of which is not what it appears to be – a seemingly innocuous piece of code, inside which lies the electronic equivalent of the Greek army *élite*, just waiting to leap on your unsuspecting computer with weapons at the ready.

Alas, things are not always this clear, which is why I prefer the term 'non-viral malware'. The word 'Trojan', even within the computer security field, has historical implications which are best avoided.

Terrifically Timely Threat?

The first question that springs to my mind with regard to Trojans is 'Why now?'. That is to say, why is non-viral malware a problem at this point in the history of undesirable software? Often the answer to this type of question is 'it has only just become possible to write this sort of program'. *Word* viruses only became a problem when *Word* included a powerful programming language. On the face of it, this does not seem to apply to non-viral malware – surely it has always been possible (indeed, easy) to write such things? Of course it has, but the technical advance that causes the perceived new threat has come not from the authors but from the operating system and application developers. It was inevitable.

AOL – Where Innocents Play

America On-Line is the service that has brought the wonders of a connected world to the masses. Millions of subscribers [*12 million, according to the* AOL *web page. Ed*] are able to inhabit a bewilderingly extensive universe of chat rooms and discussion forums, all of which exist within the silicon walls of the *AOL* mainframes. It seems impossible to purchase a mass-market computing publication anywhere on the planet without it having a free *AOL* CD on the cover, with the associated 50 free hours.

Many of the people that make up the *AOL* user community know almost nothing about computers – that is the beauty of the system. All you have to do to get online is insert the CD, and the wonders mentioned above are available to you.

Also available to you are the hazards. 'Trojans' are allegedly rife on *AOL* – binaries sent to unsuspecting users which, when run, seize their login details and send them to the author. The *cognoscenti* report that they have collected many dozens of this type of program, with more appearing all the time. Anyone with a copy of Visual Basic can produce such a program in a matter of hours, at the most. It would be easy to label this folder '*AOL* only', and slide it into a dusty cabinet somewhere in the basement. However, things are moving fast now, and this would be a mistake.

The World Inside Your Windows…

AOL was targeted, as mentioned above, because of the innocence of the users and the ease of attacking the user interface. It has not taken people long to realize that much the same is true of *Windows 95*. We are now seeing non-viral malware that attacks *Windows 95* dial-up networking, seizing telephone numbers and login details. It would not be unreasonable to expect both more of the same and new attacks in the future.

In spite of all this background, the 'why now?' question is still out there. Readers will have realized that the answer has been right in front of them as they read the above paragraphs. Communication using computers, and the integration of their operating system with the communication media, is removing the need for malware to replicate itself. The replication medium is available to the authors without any extra effort – the Internet, and the networks

that join it, will transmit the malware without the author having to expend any undue effort in that direction. In addition to this, the importance of the tremendous homogeneity of the modern desktop environment should not be underestimated.

The present situation is such that if someone writes a piece of malware, they can transmit it across the Internet by any one of a variety of means, and rest assured that people will obtain and execute it, on an operating system that will almost certainly be *Windows 95*, *98*, or *NT*. Replication code would be a waste of effort.

How to Test a Trojan

Consequently, products commonly prefixed with 'anti-virus' are having detection routines for non-viral malware added. This, in turn, results in the need to test how well they live up to their claim to defend against such things – to evaluate the effectiveness of the attempted solutions. Therein lies the problem.

Creating a test-set of viruses against which to test products is, comparatively speaking, easy. The tester must obtain virus samples, ensure that they are indeed viruses (by replicating them), and create valid replicants which are categorized and added to test-sets. It is time-consuming, and at the same time difficult and dull, but this verification process can, and must, be done.

There are many technical difficulties inherent in the above process – many viruses will not replicate easily, many more will only replicate on very specific systems, and under very specific conditions. None-the-less, they must all replicate. If one does not, then it is not a virus.

When the programs in the tester's test-sets are non-viral, however, how can this verification process possibly take place? With viruses, there is one definite condition that must be met. With non-viruses, there are no such certainties, nothing separates an innocuous copy of VI.EXE from a version of the same program with a trigger (of any type, not necessarily destructive) concealed deep inside.

Which returns us to a less obvious, but more fundamental question. What makes a program malware? It is important to attempt to resolve this question – how else are we to know how to update detection algorithms appropriately?

Indecipherable and Undefinable?

We may arrive at a formalized, mathematical definition that will assist in an answer to that question. Formal software proof is not a field in which I feel comfortable, but I believe that no knowledge of formal definitions is required to see the fundamental problems with such an approach.

Imagine you are an innocent when it comes to computers. One day, in your email, you receive a program. Your advanced, late 1990s email client silently undertakes the tedium of decoding, and presents you with a tempting icon labelled 'SEXYPICS.COM'. Above the icon is a message describing the dubious delights that will be yours just as soon as you double click. As soon as you do, however, a command prompt appears with an unintelligible message. You hit keys randomly, and suddenly unpleasant things start happening to your hard drive – before you really know what is going on, your data has disappeared.

So? It's a Trojan, right? You should have been running anti-virus software (with non-viral malware detection), and this would never have happened. Well, even if you were, it could not possibly have been expected to pick this up, because the truth of the matter is that my imaginary creation SEXYPICS.COM is nothing more than a renamed copy of FORMAT.COM from your version of MS-DOS. The unintelligible question was the 'Are you sure?' query, but either you were not concentrating, or perhaps it was in a foreign language.

In spite of the fact that this example is unlikely to happen in reality, my point is made. FORMAT.COM is, under normal circumstances, a perfectly innocent program that just happens to do 'damage'. That does not make it a Trojan, non-viral malware, or any such thing! However, package it differently, wrap a harness of spin around it, and then it is non-viral malware…

The conclusion is inevitable – Trojans cannot be identified simply by looking at the bytes that make up the binary. No amount of mathematical analysis or formalized description can avoid this simple, unavoidable conclusion; those intent on validating their tests this way are doomed to fail. They may reach an 'answer', but it cannot possibly help.

Testing Techniques

Where to go from here? Clearly, it is necessary for products that claim to offer some form of protection against non-viral malware to be tested against that claim. At this time, the University of Hamburg is the only organization that is attempting such tests. The criteria for placing a sample of non-viral malware into the Hamburg test-set are far from clear – they have been the subject of some debate of late, and are still shrouded in mystery. Persistent questions asking how to submit SEXYPICS.COM as a piece of malware are met with silence.

Regardless of the concealed specifics of Hamburg's system, it is clear that if such tests are to continue, some form of best practice for non-viral test-set maintenance is required. Simply throwing everything anyone claims is malware into the virtual pot is, quite obviously, not enough.

Conclusion

It is always a disappointment, in intellectual terms, not to have an answer for this type of question. My opinion is that there seems to be no solution to this particular problem. I look forward, without much hope, to being proved wrong.

COMPARATIVE REVIEW

NetWare You Wanted to Go?

It is now sixteen months since *Virus Bulletin* published its last *NetWare* comparative review. The hope was that the much-anticipated release of *NetWare 5.0* would have happened in time for this to be *VB's* first review based on that platform. Unfortunately, as seems to be common with major operating system upgrades, the *NetWare 5.0* release has been further delayed. The product submission deadlines could not be however, so, in late April, eleven developers shipped their current *NetWare* server offerings to our Abingdon office.

This number is down somewhat on the previous *NetWare* comparative. Several vendors indicated they were close to releasing 'much improved' versions for this platform (or, more specifically, for *NetWare 5.0*) and would prefer not to have their current versions tested.

Testing Procedures

Apart from the 'standard' tests of on-demand detection, where the scanner is pointed at the combined test-sets and allowed to run, on-access or real-time detection rates were also measured. This was achieved by running a utility from a workstation that recursed the test-set directory tree, attempting to open every file encountered along the way. For this test, the scanners were configured for on-access detection, as the test utility only tries to open, not write to, the files. (Full 'on-access' scanning is the default setting for very few realtime scanners. For performance reasons just 'on write' or 'on modify' settings are more typical, and for most production systems quite sufficient).

With the increasing dependence upon on-access scanning, a high detection rate alone may not be enough. A product whose on-access component imposes a heavy performance hit on a server will not be highly sought after. Thus, an effort was made to measure the overhead of the various on-access scanning options.

This was achieved by timing how long it took to copy 49 EXE files (all those from SYS:PUBLIC) from one server directory to another. The *NetWare* NCOPY utility was used as it keeps the transfers internal to the server, significantly reducing variations inherent in network transfers. Following a baseline condition, in which the test was run just after a server restart and with none of the scanner components loaded on the server at all, each of the available options and combinations were tested. Each test condition was repeated ten times and the average is reported.

Disk caching can affect the results of such tests dramatically. To reduce such effects in these tests, two runs, whose times were not recorded, were made immediately before each set of ten tests was run. In addition, under baseline conditions one complete test cycle was made and the results discarded before running the actual baseline test.

It seems that many users rely too heavily upon on-demand scanning (at start-up on workstations and scheduled on workstations and servers). Thus, it is with some reservation that the results of the following tests are reported, lest their inclusion should in any way unduly strengthen the perception that on-demand scanning is significantly important.

To measure the speed of the on-demand scanners, the *Virus Bulletin* Clean test-set was copied to a directory on the server and a 'manual' scan run and timed. To nullify any spurious caching effects (which should be small on a 5500 file, 520 MB test-set anyway), the server was downed and restarted immediately before running these tests.

All timed tests (speed and overhead) were run with just the server and one workstation connected via a hub. The workstation was logged into the server as the *NetWare* Admin user. 'Remote' administration programs were not run during any of the speed tests. However, as these were often the only method of changing the realtime scanning settings for the overhead tests, such programs were run at the connected workstation between test conditions, then shut down while the tests ran. The overheads are presented in percentage terms in the results table and normalized to a ten second baseline in the graph of overhead results.

In general, the suggested installation defaults were accepted. Two exceptions were made to this – offers to scan the server during or straight after setup, and requests to modify the server's AUTOEXEC.NCF file, were declined.

Test Sets

The 'usual' *Virus Bulletin* test-sets were employed, with the exception of the In the Wild Boot set, as boot infector scanning is not directly relevant to NLM-based products. The BIOS and DOS routines 'underlying' *NetWare* are completely cut off once the server loads, so any viruses present there will not affect the server (unless they corrupt something during the machine bootstrap or server load phases). Some products offer the option of scanning the DOS memory of the server anyway, providing a chance to raise a warning should there be something of concern run during your server boot process.

This does not mean that *NetWare* servers are 'immune' to boot viruses – we hear too many tales of woe about infected diskettes and/or long-term infections of some payload-toting virus where the affected server happens to be rebooted one too many times or on the 'wrong' date. Avoiding these kinds of problems, or even warning you of them, is not something a *NetWare*-hosted scanner can

On-demand tests	ItW File		Macro		Polymorphic		Standard	
	Number	%	Number	%	Number	%	Number	%
CA Cheyenne Inoculan	666	100.0%	1085	93.0%	13489	99.0%	921	100.0%
Command AntiVirus	666	100.0%	1162	99.3%	13499	99.1%	921	100.0%
Cybec Vet NetWare	658	99.4%	1114	95.4%	13498	99.1%	916	99.4%
Data Fellows FSAVN	666	100.0%	1162	99.3%	13500	100.0%	921	100.0%
Dr Solomon's AVTKN	666	100.0%	1162	99.3%	13500	100.0%	921	100.0%
Intel LANDesk Virus Protect	666	100.0%	1146	98.0%	13500	100.0%	921	100.0%
Kaspersky Lab AVPN	666	100.0%	1162	99.3%	13500	100.0%	921	100.0%
Norman FireBreak	666	100.0%	1132	96.8%	13495	99.0%	921	100.0%
Sophos SWEEP	666	100.0%	1158	99.0%	13500	100.0%	917	99.4%
Symantec Norton AntiVirus	666	100.0%	1142	97.7%	13500	100.0%	921	100.0%
Trend Micro ServerProtect	623	91.9%	902	77.2%	12411	90.2%	881	96.5%

reliably do. The long and short of this is that these scanners are not run against the In the Wild Boot test-set, so the *VB 100%* awards are based solely on results against the In the Wild File test-set.

The other interesting thing to note is that, since the last review, the Macro test-set has been augmented with samples of the first *Microsoft Access 97* macro viruses. A few vendors were claiming detection of these within days of their appearance in mid-March, so it will be interesting to see how many had built this capability into the product they were shipping in late April.

So, how did the eleven products stack up? Let's find out...

CA Cheyenne Inoculan v4.0

ItW File	100.0%	Macro	93.0%
ItW File on-access	100.0%	Macro on-access	93.0%
Standard	100.0%	Polymorphic	99.0%

Following initial problems with installing the product because a licence key was not provided with the review copy, proceedings picked up greatly. *Inoculan* displayed some admirable detection gains over recent *Virus Bulletin* test results, particularly against the Polymorphic and In the Wild File test-sets, attaining its first VB 100% award for the latter performance. On the Macro test-set, 93.0% is a little disappointing, and somewhat surprisingly it was mainly *Word 7* viruses that caused *Inoculan* trouble.

The *Inoculan* approach to anti-virus issues is to provide tools for the centralized management of server scanning and workstation deployment and management. To this end an administration program is run from a workstation to configure and monitor the server-based scanner.

Although replete with configuration options, several 'features' of the user interface of the management program are truly irksome. Spin-dials are great interface gadgets for the mouse-bound, and are normally quite tolerable to keyboarders. However, when you cannot type entries into them – particularly when the intention is to maximize the log file size from its default of 100 lines to its upper limit of 32,767 – they rapidly become a major annoyance. All the spin-dials in *Inoculan* need to be fixed! A quick search for the file holding the log file configuration options and some trial-and-error editing saw this 'problem' resolved in time to make the review copy deadline.

A configuration option involving special handling of certain server I/O calls, including those generated by NCOPY, caused some problems in the overhead tests. The product worked fine, but reliable timing data could not be recorded

On-access tests	ItW File		Macro		Polymorphic		Standard	
	Number	%	Number	%	Number	%	Number	%
CA Cheyenne Inoculan	666	100.0%	1085	93.0%	13489	99.0%	921	100.0%
Command AntiVirus	666	100.0%	1162	99.3%	13499	99.1%	921	100.0%
Cybec Vet NetWare	658	99.4%	1114	95.4%	13498	99.1%	915	99.3%
Data Fellows FSAVN	666	100.0%	1162	99.3%	13500	100.0%	919	99.7%
Dr Solomon's AVTKN	666	100.0%	1162	99.3%	13500	100.0%	921	100.0%
Intel LANDesk Virus Protect	666	100.0%	1146	98.0%	13500	100.0%	921	100.0%
Kaspersky Lab AVPN	666	100.0%	1162	99.3%	13500	100.0%	919	99.7%
Norman FireBreak	666	100.0%	1132	96.8%	13495	99.0%	921	100.0%
Sophos SWEEP	666	100.0%	1158	99.0%	13500	100.0%	917	99.4%
Symantec Norton AntiVirus	666	100.0%	1142	97.7%	13500	100.0%	921	100.0%
Trend Micro ServerProtect	623	91.9%	902	77.2%	12411	90.2%	881	96.5%

for test conditions that involved intercepting file write operations. Of the five false positives recorded against the Clean test-set, three were for the 'Texas' virus.

Command AntiVirus for NetWare v4.50β

ItW File	100.0%	Macro	99.3%
ItW File on-access	100.0%	Macro on-access	99.3%
Standard	100.0%	Polymorphic	99.1%

This beta version of *Command AntiVirus for NetWare* (*CSAVN*) sees the long-awaited *F-PROT v3.00* detection engine first come under scrutiny in a *Virus Bulletin* test. The new engine certainly exhibits the much-needed detection improvement that has been promised for so long. Perhaps not surprisingly, there is a particularly noticeable improvement over recent *CSAV* and *Command F-PROT Professional* results in the Polymorphic test-set.

As noted in the recent standalone review of *CSAVN* (see *VB*, March 1998, p.21), the name transition is not complete throughout the product. In some places the name 'F-PROT' appears, whereas in others the reference is to 'CSAV'. This continues through the documentation and on-line help, but will hopefully be corrected by the time this product completes its beta phase.

Installation is performed by the near ubiquitous (in the *Windows* world) *InstallShield*. Server components are copied to SYS:SYSTEM and a *Windows*-based administration program is installed to the workstation.

Across the other products in this review there is an either/or approach to administering the server-based scanner – it is either all done at the server console (and thus can be remotely managed via RCONSOLE) or all done with workstation-based administration tools. Neither is really 'right' or best for everyone.

The designers of *CSAVN* acknowledge this by allowing virtually full administration from the server console (by extending the server's command set with a range of CSAV commands) or from a workstation-based administration program. The only possible addition we could suggest is the inclusion of a scripting capability, though we are prepared to concede that there may in fact be one there already – being a beta, the software still had a few rough edges, but the documentation was lagging well behind!

CSAVN was certainly not the fastest product in the round-up, and the overhead imposed by its on-access component was also very high. Being a beta version, it may be too early to make definitive statements about such performance issues, but potential purchasers should check this carefully when the product is released.

	Overhead				Scanning Speed		False Positives
	Loaded Inactive	Read or Outgoing	Write or Incoming	Read and Write	Time (min:sec)	Throughput (KB/s)	
CA Cheyenne Inoculan	25.0%	35.7%			21:01	423.6	5
Command AntiVirus	17.1%	88.4%	127.5%	122.1%	54:49	162.4	1
Cybec Vet NetWare	-1.5%	33.0%	28.2%	29.9%	9:07	976.4	12
Data Fellows FSAVN	4.8%	56.4%	44.7%	49.2%	17:22	512.6	4
Dr Solomon's AVTKN	-2.7%	109.5%	71.1%	147.9%	39:47	223.8	0
Intel LANDesk Virus Protect	9.0%	6.1%	45.6%	44.4%	15:41	567.6	0
Kaspersky Lab AVPN	4.6%	46.8%	34.6%	43.7%	17:40	503.4	4
Norman FireBreak	0.2%	5.6%	25.2%	31.0%	13:03	682.1	0
Sophos SWEEP	-1.6%		34.4%	89.6%	12:00	741.8	0
Symantec Norton AntiVirus	0.7%	59.4%	58.5%	68.3%	7:01	1268.7	0
Trend Micro ServerProtect	4.8%	41.9%	45.9%	48.8%	25:47	345.3	3

Cybec Vet NetWare v9.70

ItW File	99.4%	Macro	95.4%
ItW File on-access	99.4%	Macro on-access	95.4%
Standard	99.4%	Polymorphic	99.1%

Since *Virus Bulletin* last reviewed this product it has experienced a name change (see *VB*, October 1997, p.18). The developers have added email and SNMP trap alerting methods. Installation must proceed from a PC running *Windows 95* or *NT*, and looks much like other *Vet* setup routines. An option common to many products in this review is the ability to select multiple servers and concurrently run the same installation or update on all of them.

A twist to this, unique to *Vet*, is that at the end of the setup process you can return to the server selection list and choose another set of servers to receive a different configuration, and so on, avoiding repeating the first part of the setup rigmarole. Apart from this multi-server installation option, there appear to be no facilities for grouping multiple servers into management 'domains' nor for automating updates across or between servers.

Immediate scans default to 'blind' scanning mode, whereas on-access scanning defaults to 'intelligent' mode. This explains why, in the on-access test, *Vet* missed the same viruses as on-demand plus a Midin.765 sample – the 'blind' scanner would run across this mid-infector regardless of where its code ended up in the host, whereas the 'intelligent' scanner would only catch infections where the code happened to fall in an area considered 'important to scan'.

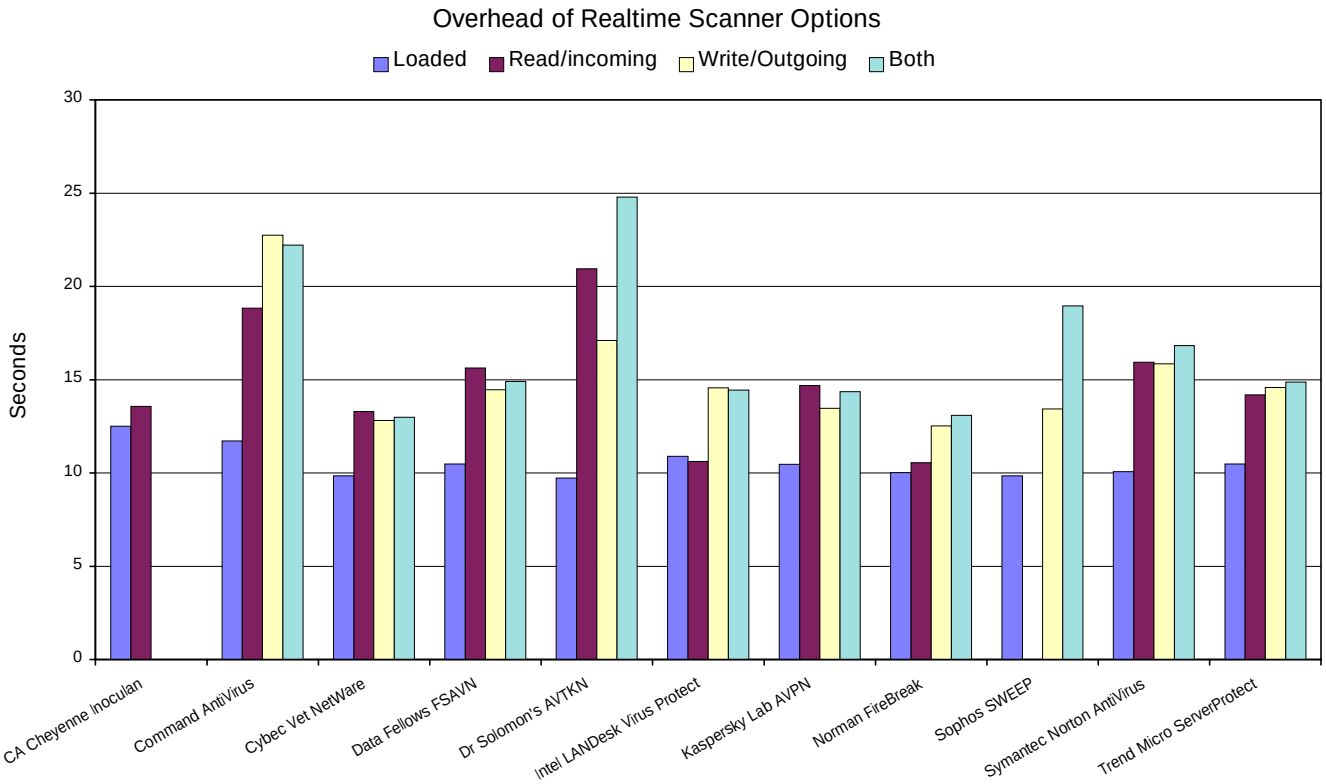
Vet's on-demand scanning speed was considerably faster, with a throughput of 2234.8 KB/s, if set to 'intelligent' mode for that test. The false positives were all of the HLLO.40932 virus, suggesting a poorly chosen scan string – the developers claim this is now fixed.

Data Fellows F-Secure Anti-Virus v4.00

ItW File	100.0%	Macro	99.3%
ItW File on-access	100.0%	Macro on-access	99.3%
Standard	100.0%	Polymorphic	100.0%

As with their DOS scanner, included in the February 1998 comparative, *Data Fellows' F-Secure for NetWare* (*FSAVN*) uses only one of the two engines the company licenses – *AVP* from *Kaspersky Lab*.

In fact, the product is essentially a re-badged *AVP for NetWare*. A readme file supplied with the product promises a *Windows*-based administration client 'in an upcoming release', but in the meantime you still need a *Windows 95* machine (running *Client32 – Novell's* 32-bit *NetWare* client for *Windows 95*) to run the installation program. A unique



feature (within this review group) was that at the end of the brief installation process, the scanner was auto-loaded on the server. Beyond this, functionality and performance were identical to *AVP for NetWare*, and the reader is referred to that product's review section for more details.

Dr Solomon's AVTK for NetWare v7.83

ItW File	100.0%	Macro	99.3%
ItW File on-access	100.0%	Macro on-access	99.3%
Standard	100.0%	Polymorphic	100.0%

Although still at the head of the pack in terms of virus detection, the rest of *Dr Solomon's Anti-Virus Toolkit for NetWare* (*AVTKN*) seems to be suffering a serious case of arrested development. Compared to *InstallShield*, INSTALL.BAT hardly sets the image of a product for the late 1990s.

The complex and potentially powerful configuration scripts are still present, yet the simple, *Windows*-based configuration editor displays its lack of currency with a message in the Help/About box saying 'Copyright (C) S&S International PLC 1995'.

Worse, there was three-way discrepancy with regard to the on-line help, the printed documentation and the interface of the reviewed product. This was particularly noticeable in configuring the realtime component of *AVTKN*. File Access Monitor v7.83 wishes to disinfect by default, yet this is not even mentioned as an option in the documentation or on-line help. 'Unconfiguring' this option was quite a battle.

Nor did the configuration editor hint that an option it did not understand was the preset default. Further, none of the 'intuitive' options that were tried in manual editing of the configuration file worked either. In the end a setting of 'Alert on Reads, Rename on writes' was the nearest setting to the desired 'report only'.

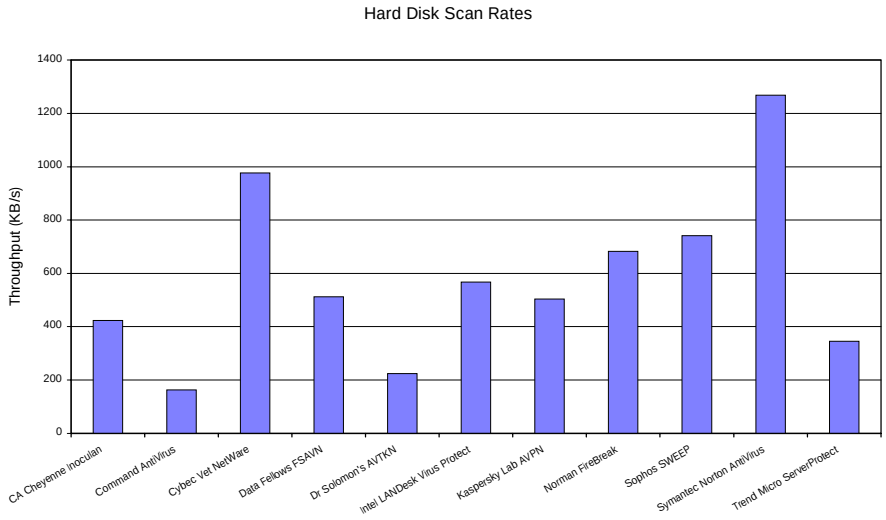
The clunky interface aside, *AVTKN's* detection performance left little to be desired, only missing the four samples of each of the *Access 97* macro viruses. Speed and overhead were not stunning, but *AVTKN*, by default, pauses briefly between files it scans so as not to hog the CPU. This can be disabled for on-demand scanning and doing so resulted in throughput improving to 355.1 KB/s.

Intel LANDesk Virus Protect v5.02

ItW File	100.0%	Macro	98.0%
ItW File on-access	100.0%	Macro on-access	98.0%
Standard	100.0%	Polymorphic	100.0%

Apart from signature updates, this is the same version of *Intel LANDesk VirusProtect* (*LDVP*) reviewed in the February 1998 issue. Readers are referred to that review for details of *LDVP's* functionality. In brief, this is a full-featured product, from the network manager's perspective, and this version leaves little to be desired from that quarter.

An *LDVP*-protected server can automatically update from another server within your organization or from the Internet (via FTP) or a BBS. Checking these sources for updates can



be scheduled, although only one source can be configured as 'active'. Domains of like-configured workstations and servers can be controlled centrally. Workstation settings can be 'locked' to prevent fiddling fingers interfering with your corporate anti-virus policy implementation.

A *Windows 95* or *NT* workstation is required for the installation and administration. *LDVP* now incorporates the *IBM* anti-virus engine, perhaps accounting for the significant detection gains evident here.

Kaspersky Lab AVP for NetWare v3.0

ItW File	100.0%	Macro	99.3%
ItW File on-access	100.0%	Macro on-access	99.3%
Standard	100.0%	Polymorphic	100.0%

Kaspersky Lab's product continues its tradition of high detection rates, albeit at the cost of raw speed. *AVP for NetWare* (*AVPN*) and its *Data Fellows FSAV* incarnation were the only products to detect any of the *Access 97* viruses in these tests, finding all four A97M/AccessiV.A samples.

Another product taking a minimalist approach, *AVPN* is installed through the simple expedient of perusing a readme file then copying the appropriate files to a suitable directory on the server. Should you elect to install *AVPN* in a differently-named folder from the suggested default, a few minor tweaks will need to be made to the supplied NCF loader script, and then it is ready to run.

There are neither network-wide management tools nor mechanisms for distributing signature database updates from one server to another. Although the NLMs do not need to be unloaded from the server to activate signature updates, you must manually activate such updates from a menu. This can be achieved remotely via RCONSOLE.

The default settings for the on-line scanning option include scanning only COM and EXE files. For the purposes of fair testing, this was changed to all files (*.*) – the same as the default for on-demand ('manual') scans. This non-default setting was used for all on-access tests, including those of scanner overhead.

The on-line scanner was overwhelmed by the on-access test procedure. Its report files indicated finding approximately 10% of the total test-set, and most of these detection reports were duplicated in the report files.

After several unsuccessful attempts to cajole *AVPN* into better co-operation, it was configured to delete infected files and the file access process was modified to recurse the test-set directory tree repeatedly, attempting access to each file found there. This was left running overnight and when the scanner was clearly not deleting any more files the test was deemed to have reached completion. Four false positives were reported in the Clean test-set.

Norman FireBreak v3.86

ItW File	100.0%	Macro	96.8%
ItW File on-access	100.0%	Macro on-access	96.8%
Standard	100.0%	Polymorphic	99.0%

Variously labelled *Norman Virus Control for NetWare* and *Norman FireBreak*, this Norwegian product reaffirms *Norman's* recent record of very good detection performance in *VB* tests.

A *Windows* client PC is required for the installation of *Norman FireBreak*, due to its use of *InstallShield*. Apart from this, the product seemed to be a fairly traditional *NetWare* console application, with no remote administration software or the like. Unloading of the NLM and access to its configuration menu can be password protected, but this option is not set by default. Either way, you cannot unload the NLM from the System Console but only from the *FireBreak Console*.

FireBreak can be configured as a 'communications hub'. In a multi-server network, such a hub becomes a central point to which other, suitably configured, *FireBreak*-protected servers can send virus incident reports. Beyond this centralized reporting, logging and alerting capability however, *FireBreak* does not seem to provide for multi-server management or LAN-wide updating. Somewhat confusingly, several of the menus refer to 'manual/scheduled' scanning, but there was no apparent mechanism for configuring scheduled scanning – something of an odd omission in a server product.

Similarly to *Dr Solomon's AVTKN*, *FireBreak* provides a command-line option to remove its inter-file scan delay. This could be handy for speeding up scans when the server is not under a heavy load, such as in the evenings or at

weekends before a backup is due to start. Utilizing this option and repeating the throughput test resulted in a slightly better performance of 809.3 KB/s.

Sophos SWEEP v3.09

ItW File	100.0%	Macro	99.0%
ItW File on-access	100.0%	Macro on-access	99.0%
Standard	99.4%	Polymorphic	100.0%

SWEEP has a very simple installation procedure – copy the supplied NLM to the server (preferably to the SYS:SYSTEM directory). You have to do this 'manually'. It seems that the effort of writing an installer to copy just one file has, perhaps unsurprisingly, been deemed not worthwhile by *SWEEP's* developers.

Actually, this comment is a little unfair – on first loading *SWEEP* on the server, it detects that it has not run before and sets itself up. This includes making a 'home' directory for itself, and others in which to 'quarantine' infected files and to manage the server side of its interface to *InterCheck* (should you choose to use this machine as an *InterCheck* server for your workstations). It also installs a number of other files that are packed inside the main NLM.

Since last reviewing this product, some basic update management facilities have been added. *SWEEP* can now be configured to look for an upgraded NLM in a directory on the server, and when one is detected, it will unload itself and load the new one (this process has some integrity checks built into the replacement NLM). There is also a companion NLM allowing 'remote scripting' control of the console command line.

Although claiming NDS awareness, in testing *SWEEP*, it seemed unable to consider objects to scan other than at the volume, directory and file levels. It could be configured to ignore objects at the directory and filename levels, though wildcards are not allowed, potentially limiting its usefulness. The extent of *SWEEP's* NDS awareness appears limited to selecting NDS user groups for alerting purposes.

The scanning speed reported is for *SWEEP's* first run, in which it creates checksums for *InterCheck's* use (whether you use *InterCheck* in client-server mode or not). A subsequent run returned a throughput of 989.1 KB/s.

Symantec NAV for NetWare v3.xx

ItW File	100.0%	Macro	97.7%
ItW File on-access	100.0%	Macro on-access	97.7%
Standard	100.0%	Polymorphic	100.0%

Symantec's Norton AntiVirus (*NAV*) was yet another product using *InstallShield*, which installed the server scanner and workstation-based administration components. On detecting it was installing to a *NetWare 4.1x* server, the option of adding a *NAV* 'snap-in' to the *NetWare Administrator* program was offered.

Missing the *Access 97*, and a small number of recent *Word 97*, macro viruses, *NAV* continues on its course of improved virus detection.

Trend Micro ServerProtect v3.51 VPN 362

ItW File	91.9%	Macro	77.2%
ItW File on-access	91.9%	Macro on-access	71.2%
Standard	96.5%	Polymorphic	90.2%

Another product aiming to be a complete network anti-virus management solution is *Trend's ServerProtect for NetWare* (*SPNW*). It has a graphical installation routine, workstation-based administration and very minimal functionality or configurability at the server console.

Various server and workstation components display copyright notices mentioning *Intel* as well as *Trend Micro*, and the general look and feel of the product suggests something of an older version of *Intel's LANDesk Virus Protect*. Indeed, much of the terminology, and even the default domain protection password, is the same.

Unfortunately, instability in the review copy led to very low detection rates. The patch shipped to fix this resulted in some of the previously detected viruses (including the *Access 97* macro viruses) not being detected. Use of a significantly newer virus signature file improved detection dramatically, but inclusion of those results would unfairly disadvantage the other products in this review.

Conclusion

As far as feature sets go, the tested products clearly cover a broad range. At one end of the spectrum are the simple single server scanners, controlled from the *NetWare* system console. Apart from detecting viruses, these have little in common with the 'Starship Enterprise' models that allow for a single point of management and update for all servers (often *NetWare* and *NT*) and all common desktop machines within the organization.

It is encouraging to note the continuing improvement in overall detection, although it should be remembered that a somewhat depleted set of products has been tested.

Technical Details

Hardware: Server – *Compaq Prolinea 590*, 90 MHz Pentium with 80 MB of RAM, 1 GB hard drive, running *NetWare 4.10* with LIBUPG and 410PT8B applied. Workstation – 166 MHz Pentium with 4 GB hard drive and CD-ROM drive, running *Windows 95* with *Novell's Client32*.

Test Sets: Complete listings of the test-sets used can be found at http://www.virusbtn.com/Comparatives/NW/199807/test_sets.html. Note that this listing includes the In the Wild Boot test-set although it was not used in this review.

PRODUCT REVIEW 1

Defuse Enterprise for Word

This review is something of a novelty for *VB*. *Defuse Enterprise*, from *Portcullis Computer Security Ltd*, concentrates on *Word* macro viruses, while claiming to protect against all macro malware for *Word* – still a narrower field than many of the sprawling anti-virus suites reviewed in the past. It might be expected that such a one-track product would be a master of its trade – a hypothesis which *Virus Bulletin* set about testing.

Packaging and Documentation

Defuse was supplied on six floppies, three of which cater for the administrator, two the user and one for uninstallation. The contents of this last diskette consisted of two document files containing macros for use in the uninstall process under either *Word 8*, or any previous versions, respectively. The six diskettes were accompanied by an A4 manual of 37 pages but, in a break from the norm, no box.

The manual starts with descriptions of the possible threats that macros can pose. This proved to be an interesting read, categorizing said threats as letterbombs, timebombs, spies, interlopers, data kidnappers, firewall-hoppers, password crackers and finally viruses. Their implications and possible attack methods are delineated, leading to a more technical discussion of infiltration techniques used in macros for the subversion of normal activity.

The manual advises that the average user is denied access to this material, and indeed some of the ideas included might be dangerous in the wrong hands. As the manual states, however, this information is freely available to those who know how and where to find it.

The remaining bulk of the manual is devoted to more technical issues such as configuring and administrating the product. These activities are covered in good detail, with considerations provided for most of the choices. It is also clear that the program's author is aware of the evil or foolish nature of some users, and possible security issues, together with their solutions, are addressed as they arise.

Defuse uses a method which analyses macros present in a document, and then presents an overall judgement of the potential hazards. These security threats are rated in a numerical system. There is also provision of several reports generated by the Macro Analyser, of which more later. From all appearances, the application consists partly of a number of DLLs and partly of a selection of macros.

Defuse is available for *Word 6/7* and *Word 97* running under *Windows 3.x*, *OS/2*, *Windows for Workgroups*, *Windows 95* and *Windows NT* as appropriate. It is not known whether a Macintosh version of *Defuse* is in the pipeline, but the developers are working on a version for *Excel* which they hope to have completed by September of this year.

Installation

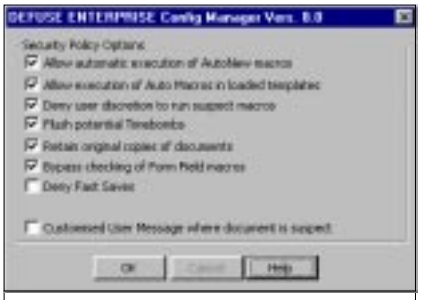
Installation was first tested on an *NT* 4.0 SP3 standalone machine, installing into *Word 7.0a*. *Word* had been installed as part of the *Office 95* suite, under the default setup configuration for that package. This installation was performed using the administrator disks. It was intended that later installations would use this copy of *Word* as the central network path, as is required for correct and secure administration of *Defuse*.

The installation process appeared to go smoothly, and a pair of bars showing levels of CPU and RAM usage gaily zipped up and down as the Administrator disks were processed. The installation utility demanded to be fed with 'installation disk 2', rather than 'administrators disk 2', but the true meaning was easy to discern. The applications installed consisted mainly of DLLs, which found their way into the appropriate WINNT40\System directory.

After installation a dialog box appeared, only to be instantly hidden by another. The obscuring box was definitely designed to be in the way, as it requested that any existing *Word* sessions be shut down. When clicked away, the hidden box proved to be a message that *Word* was now being updated 'in the background', and should be restarted to complete installation.

Word ground through its startup, opening and closing documents aplenty, before a new dialog box appeared – part of the main Configuration Manager. From here Installation Options, Security Policy and Incident Reporting choices were offered, though the defaults were chosen for this first installation. Then *Word* was exited in order for *Defuse* to complete its setup. It was here that problems arose.

Word, whilst shutting down and executing *Defuse's* macros, caused an error due to a missing document. This document, which went by the name of V7BUTTON.DOC, was assumed, correctly, to be part of the *Defuse* suite.



The administrator can enforce these options upon *Defuse* users.

Investigation turned up an installation log file in the 'temp' directory. This logged all DLLs and documents, with the exception of two, as having

```
DEFUSE ENTERPRISE Vers. 8.0a
SUSPECT DOCUMENT REPORT - CRTMNA-1.DOC

SUMMARY OF FINDINGS.

1: Embedded code will run.
2: Document carries a Payload.
3: Imports macro code.
4: Conceals its actions.

Definitely do NOT open!!

FIRST-STAGE ANALYSIS of crtmna-1.doc

Contains the following macros:

…

 Contains code which will automatically execute:
 Will hijack Word commands:
 Attempts to subvert analysis:

Non-standard System Command, Menu, Toolbar and Key Assignments

 8 replaced System Command macro(s)
 0 non-standard menu item macro(s)
 0 non-standard toolbar button macro(s)
 0 key(s) assigned to non-standard macros.

"Cartman.FileClose" replaces the System Command Macro.
"Cartman.FileExit" replaces the System Command Macro.
"Cartman.FileNew" replaces the System Command Macro.
"Cartman.FilePrint" replaces the System Command Macro.
"Cartman.FileSave" replaces the System Command Macro.
"Cartman.FileTemplates" replaces the System Command Macro.
"Cartman.ToolsMacro" replaces the System Command Macro.
"Cartman.ViewVBCode" replaces the System Command Macro.

RESULTS OF THE CODE ANALYSIS

Analysis of Cartman.AutoClose Macro

Runs the following macro:
"    Call Cartman"

Analysis of Cartman.Cartman

Danger! CARTMAN.CARTMAN will copy a =TWO$, NAME:="CARTMAN",
OBJECT:=WDORGANIZEROBJECTPROJECTITEMS macro from
application.organizercopy source:=one$ into NORMAL.DOT
Organizer command may modify a macro on your system
May attempt to write to or modify the Startup Path!
Switches off prompt to save changes to normal.dot
FileSaveAll may be forcing save of changes to the global template.
Disables Word macro virus protection.
Runs the following macro:
"    If nfat = vbReadOnly Then Call vBitchES(msfile$)"
Runs the following macro:
"    If nfat = vbReadOnly + vbArchive Then Call vBitchES(msfile$)"
```

Partial output from the Macro Analyser.

been installed to the correct directories. V7BUTTON.DOC and a second copy of DEFUSE.HLP had been installed to the root. The document was duly moved, and the Configuration Manager macro reactivated manually from within *Word*. At this point, the errors on exiting *Word* ceased and installation was assumed complete. It was notable that *Defuse* checked, at this point, for possible conflicts with other anti-virus packages.

Since problems were encountered, the Administrator install was repeated on other platforms to determine whether this glitch was more widespread. To this end, another machine running *Windows 95* SP1 and *Office Professional 97* was provided. Clearly, *Defuse* found the *Word 97* paths more familiar and the product installed on this second, hardware-identical machine more quickly and without any visible problems. Returning to the *NT* 4 SP3 platform and with *Word 97* SR-1 installed into a non-standard directory, there were again no problems, the conclusion being that the install routine does not always handle *Word 7* correctly.

Discussion with *Portcullis* traced this problem to the install having used a 'virgin' copy of *Word*, which had not yet initialized the NORMAL.DOT. Under these unusual circumstances, *Defuse* is unable to determine exactly where the V7BUTTON.DOC and DEFUSE.HLP files should be located. None-the-less, remaining tests were performed using *Word 8*, under both *NT* and *Windows 95*.

The Administrator install is only half the story if *Defuse* is to be used in a network. Individual copies of *Word* must be primed with the *Defuse* macros. The manual suggests deploying the user executable in email attachments. As the manual is not very clear at this point, there is potential for confusion. In smaller organizations, the workload should be such that Administrators could well install it upon individual machines. In a large one, however, the task would be onerous, and less technically-minded users more likely to encounter problems.

During the test procedures on other machines, the user disks were installed into *Word* directly rather than via email. If installed in this manner, the default values are used for all of the user options as regards security, messaging and installation. No further action need be taken, though in most organizations the need for security would dictate that the central Administrator's setup be used for all *Word* operations.

This central repository of configuration information is enforced by the opening of a specific document, which is produced on the Administrator's machine during installa-

tion. Non-administrator users must be given this document, and must open it. Clearly, the central *Word* startup path, containing as it does the *Defuse* macros and configuration files, must be secured from tampering if the program is to avoid alteration or subversion.

Configuration Manager

Defuse made itself conspicuous by the extra time taken to load *Word*, and documents within it. In the Administrator setup, there were also additions to the tools menu, consisting of the Macro Analyser and Configuration Manager. The latter is, unsurprisingly, the core of administration and (as mentioned) allows the control of Installation options, Security Policy and Incident Reporting.

Of these, the Incident Reporting choices are the most limited in number. The main alerting method is email directed to a single nominated address. This provides not only notification, but also the suspect document and a preliminary report on the macros in it. There is an option to write documents to a suspect directory in the administrative network drive. Either, both or neither may be chosen, though the email option only works with MAPI-compliant mail systems. There is also the choice of whether to report on macros found in NORMAL.DOT following installation onto individual machines.

The Security options menu is more extensive, and allows tweaking of the protection offered by *Defuse*. This is mainly concerned with the level at which certain macros are legitimately used within *Word*, the trust accorded to the user and speed requirements in operation. These last are addressed by allowing Form Field checks to be skipped. The third sub menu available from the Configuration Manager is the installation options menu mentioned earlier.

This last menu sets both the location of the central Network Startup path and *Defuse's* response on discovery of macros in NORMAL.DOT during installation. The option is given either to remove or ignore automacros, command replacement macros, menu item replacement macros, toolbar button replacement macros, non-default shortcut key macros or all macros. Each may be removed or saved independently, and a list of macros discovered can be sent to the Administrator. Here, too, is the option for special messages to be sent to the user if installation fails.

Macro Analyser

The Macro Analyser is a tool available only to the Admistrator, and is accompanied by dire warnings that it not be allowed to fall into the hands of any other users. When presented with macros, the Analyser provides alerts on a rating of zero (no threat) to seven (an active attack upon *Defuse* itself). Of most interest was the option to print out a report about the suspect macro, which lists macros present, redirection of *Word* commands and other handy tidbits of information. A dump of the macros in the suspect document is also available.

To a user versed in VBA, this information could be valuable in the determining of source or potential hazards involved in a macro – without having to use the easily subverted Tools/Macro route. The Analyser is supplied with an authorization tool, which may be used to pass 'false positives', known to be legitimate, as fit for use.

Detection

As neither the underlying parts of *Defuse* nor the Macro Analyser are really designed to be on-demand scanners, the standard *Virus Bulletin* testing methods fell by the wayside. Of primary interest were the macro viruses in the current WildList, which were in some cases individually analysed using the Macro Analyser tool. With traditional scanners string searches are used, and target file sizes can affect the quality of scanning, especially on-access. *Defuse's* method of analysis should be free of this complication. So, the Macro test-set was tackled with a more tester-friendly method – one sample of each virus was selected, rather than the usual selection of differently-sized documents.

It was here that *Defuse* shone, with no problems in the detection of those macro viruses with which it was presented. Although several were declared to have no payload, it was always apparent that *Word* functions were being subverted and that odd activities would result if the macro were to be run. As a somewhat harsh test, a completely new form of macro virus, W97M/Class.A was opened and also analysed. Again, *Defuse* was able to detect that something was afoot, giving a warning that the document involved was dangerous and must be cleaned.

Automatic cleaning of documents was also tested. A number of *Word 8* documents were inspected both visually, for integrity, and with a standalone scanner, for virus removal. Removal was achieved speedily and effectively, as might be hoped, with no visible problems or detectable viruses present in the cleansed documents.

With no redirection selected, it still appeared that these documents were moved to \MSOffice\Scanzone when analysed rather than opened. This left infected documents in a none too intuitive place, albeit on the Administrator's machine and, presumably, safe. With redirection selected, not only were copies sent to the Administrator's 'suspect' directory, but further copies were made in the local temporary directory, there to languish indefinitely. This occurred whether the original documents were on CD or local hard drives. The theory is that copies should be kept locally, but having a temporary directory full of viral files is far from desirable. Despite being renamed with MAL extensions, the files were still viral and detected by a standard scanner.

When the Macro Analyser was used from within *Word 7*, there was no detection of *Word 8* macros. This is no great surprise, since *Word 7* cannot make sense of *Word 8* macros, but *Defuse's* message states that scanned documents are harmless. Purists might suggest that a message should specify that there was no danger under *Word 7*.

Since viruses are not the only problems *Defuse* seeks to counter, it seemed appropriate to investigate the detection of Trojans. A small selection were subjected to the Macro Analyser's tender ministrations. A macro virus creation toolkit was detected and declared hazardous, which might be considered a false positive. The code involved operates on a user-choice basis, but this alarm cannot be faulted from an anti-virus perspective. All other Trojans were detected as being possibly hazardous, though in this test it became apparent that documents infected under the Chinese version of *Word* go undetected by *Defuse*.

Compatibility

Defuse was used in conjunction with another conventional anti-virus product so as to check for compatibility. Clearly, on-demand scanners using heuristic methods might consider that *Defuse* itself was a hostile macro, though this problem was not encountered. On-access scanning, however, interrupted the *Defuse* macro whilst it analysed the viral macro, causing *Defuse* to fail in its recognition of a potential hazard. Considering the number of anti-virus products available, compatibility between *Defuse* and any currently-used on-access scanner should be investigated by potential *Defuse* customers.

Conclusion

As a barrier, *Defuse Enterprise* is certainly effective in the detection and removal of viral macros and other hostile macros, at least in Western language *Word* versions. Small organizations or those with a high technical competence could easily implement *Defuse*, but the lack of automated distribution tools may restrict its wider use. Slight bugs during installation are, thankfully, easily avoidable.

This is a worthy product, hampered only by minor flaws in implementation. The product, so far as tested, proved effective in its major aim, with any flaws only impacting the user-friendliness and administrative ease of its use in the workplace, rather than its efficacy. Its detection of W97M/Class.A is also a timely demonstration that generic products can have advantages over pattern-based scanners, when new viral methods are first used.

Technical Details

Product: *Defuse Enterprise for Word.*

Developer/Vendor: *Portcullis Computer Security Ltd,* The Grange Barn, Pikes End, Middlesex, HA5 2EX, UK, Tel +44 181 8680098, fax +44 181 8680017, email enquiries@portcullis-security.com, WWW address http://www.portcullis-security.com/.

Version evaluated: 8.0a.

Price: 11–250 users, £20 per user; 251–1000 users, £10 per user.

Hardware used: 166 MHz Pentium-MMX workstations with 64 MB RAM, 4 GB hard disk, CD-ROM drive and 3.5-inch floppy drive running *Windows 95 (SP1)* and *Windows NT (SP3).* Several versions of *Word* were used – see the text for details.

Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NW/199807/test_sets.html.

PRODUCT REVIEW 2

ViruSweep Extra Strength for Windows 95

Quarterdeck, an old established company by PC standards, has only recently ventured into the anti-virus market. Like many other companies new to the field, *Quarterdeck* has opted to use an existing product's engine under licence – in this case that of the Israeli *EliaShim* (which trades under the name *eSafe Technologies* in other countries).

The regular *ViruSweep* was featured in *Virus Bulletin's* latest *Windows 95* comparative review (May 1998, p.10), and showed distinct similarities to its progenitor, *ViruSafe 95*, not least in the capitalization of the two product names. *ViruSweep Extra Strength* is essentially a repackaging of the *eSafe Protect* program, and the differences between the two products are fewer still.

Apart from the merest cosmetic changes, the *Quarterdeck* product is virtually identical. For this reason, readers are directed to the standalone review of *eSafe Protect* in the April 1998 issue of *Virus Bulletin* for a detailed examination of the 'vandalware' protection measures of that product. This review focuses on the parts of the package where *Quarterdeck* has made its mark and also upon the very important matters of virus detection and usability.

Packaging and Documentation

It proved something of a challenge to obtain a review copy of *ViruSweep* from *Quarterdeck*, since the organization denied knowledge of several of its own employees. Initially, it was suggested that *Virus Bulletin's* contacts might merely have been pretending to work for *Quarterdeck*, though a second, more likely, theory blamed the sprawling nature of the *Quarterdeck* empire. First impressions of the product were a little disappointing, not due to any deficiency *per se*, but because of the flimsy nature of the box, and its resemblance to a pancake on receipt. *Quarterdeck* has opted to colour-code their packaging – 'regular strength' *ViruSweep* is a bilious yellow, *Extra Strength* a virulent red. At least they are easy to recognize.

There are fewer contents than average inside the box, with a manual, CD in sealed paper sleeve and registration card making up the total. The registration card contains a short questionnaire to be returned to *Quarterdeck*, with a tear-off section providing details of the advantages of doing this and, more vitally, the registration number of the software. Registered users gain a year of virus definition upgrades.

ViruSweep Extra Strength is a more recent product than the Regular version, and the manual has been overhauled to account for both this and the addition of *eSafe Protect*. The

manual is one of the better examples of its ilk – the explanations are clear and direct, especially with reference to *eSafe Protect*, a program rife with options, sub-options and selections. Areas in which the original *eSafe* manual was unclear or lacking have been fully redressed. The overall result improves the usability of that program considerably.

As befits a company with a background in DOS applications, the command line functions of *ViruSweep's* various modules, including those for both the detection and removal of viruses, are covered in great detail. The contents of the rescue disk are also well explained. The command line programs have a number of options distinctly designed to be helpful in the production of custom batch files. Within the program itself, the on-line help is first class, with the same degree of concise accuracy applied to the results of the context-sensitive help.

Since *eSafe Protect* is designed very much with habitual Web Surfing in mind, the *Quarterdeck* website was also inspected, not least for the latest virus definition upgrade. Since *Quarterdeck* has essentially licensed the technology inside *ViruSweep* from another company, it was interesting to browse the areas relating to the *Quarterdeck Anti-Virus Research Centre* (*QUARC*).

As suspected, the information here seemed to have been gleaned not so much from in-house research but from collaboration. The Hare virus, for example, was declared removable by *F-PROT* and various related utilities – generous indeed, if this was an in-house document. There were a number of broken links on the site, notably, but not confined to, the virus library copyright page. [*The* QUARC *web site seems to have undergone a major revision just prior to this issue going to press. Ed.*]

Installation

The CD provided for review was the European release v1.0, though *Windows 95* detected it as VSESUK101. There was no Autostart provided and the root of the disk was cluttered with identity files and assorted debris totalling 37 objects and no folders. Notwithstanding, the installation process was thankfully simple. Following the usual request for name, organization and registration number, the Full or Partial installation option was presented. In this case, Partial is an install without the benefit of an on-access scanner – an option unlikely to prove very popular unless problems with speed or software clashes are encountered. The default of Full installation was chosen.

A further three Yes/No decisions were all that remained. The first determined whether the resident DOS scanner was to be initiated inside CONFIG.SYS, thus providing on-access protection in 'DOS-only' mode. Adding a desktop shortcut and an option to integrate with an installed web browser comprised the other two. All of these options were selected, again accepting the defaults. Installation was then completed in a minute or less, despite allowing a preliminary scan of the test machine to create integrity check files. After a reboot, all was ready. It was notable that the anti-virus component could not be chosen as an optional part of the package, but was installed *de rigueur*.

The Program

Installation produces a multiplicity of entries in the added Programs/ViruSweep menu. The most important part of the program, however, is more simply reached from the desktop shortcut. This consists of the standard set of tabs, accessing control over the program's settings. There are no great surprises to be had here, with the usual range of options being available. Also installed to the system tray is the *Quarterdeck Service Manager*, of more use to those with many *Quarterdeck* products and prone to crashes, and the control for on-access scanning.

Detection

As is customary, the detection capabilities of the on-access and on-demand scanners were tested against the current WildList. The version tested here was dated 28 April, and the WildList as of mid-April was used as the basis of the tests. On-demand and on-access scanners showed the reassuring ability to detect exactly the same number of viruses as one another. Scanning was stable, though it seemed to be impossible to reinstate the on-access scanner once it had been disabled, and determining whether it was indeed disabled was none too easy either.

Scanning the In the Wild Boot virus test-set proved a speedy and fairly pleasant task, with two misses out of a total of 87 samples. These were the old favourite Hare.7610 together with newcomer Lilith. Of the In the Wild File viruses, ten samples were undetected from a total of 494, a detection rate of 99%. This gives an overall In the Wild detection rate of 99%.

Of the 13,500 samples in the Polymorphic test-set, 229 were missed, with some of each of Spanska.4250, Cordobes and MTE being missed. This gives a detection rate of 95%

using the weighting method applied by *VB*. The samples of Cruncher were the only misses in the Standard test-set, giving a 99% detection rate there. Performance against the Macro test-set was the least impressive, with a total of 159 misses from 1170 samples; an overall rate of a mere 87%.

Missing any Spanksa.4250 samples is somewhat distressing, as this virus is in the wild and fairly widely distributed around the world. Aside from that, although polymorphic, it is generally coinsidered a fairly simple virus to detect.

Speed and Overhead

Since a checksummer is an integral part of the package it was deemed necessary to test the on-demand scanning speed both with and without checksum files being present. To this end, the program was installed and the option to scan the machine upon installation was rejected, assuming that this would result in a checksum free machine. This assumption was not quite correct, as further tests showed.

A first, second and third scan of the *Virus Bulletin* Clean test-set showed no increase in speed from the first – rather odd if that scan had resulted in checksum files. There were at least no false positives at this stage. Since it is possible to strip the checksum files from the machine from within *ViruSweep* this was selected as an option, and the scan was run again. This scan proved substantially more sluggish than the previous three, but a more disturbing feature was the appearance of five false positives. A further scan saw times back to their original speedy levels, but with the false positives repeated.

The most probable reason for this strange display is that *ViruSweep* applies checksums without scanning, even though the files involved may be infected and should be scanned before a checksum is produced. Despite the warning that it is advisable to scan a machine during installation, the result is a potential loophole in protection of epic proportions.

The timing tests, after the rigmarole above, resulted in data throughput of 2.5 MB/s without checksumming and 4.0 MB/s after checksums had been applied. Although not a particularly valid test of scanning rate, the on-access test of the complete *VB* virus test-set was notably faster than the on-demand test.

Another measure of performance was gained by scanning two diskettes containing identical files, though on one disk all files were infected with the Natas.4744 virus. Under this test the infected disk was scanned in 21 seconds and the uninfected also in 21 seconds. This is creditable, and reflects a speedy decision having been made by *ViruSweep* as to the viral nature of the samples.

Overhead testing of the on-access scanner was also not without its moments of strangeness. The behaviour monitor randomly triggered an alert of 'Important System Interrupts have been changed by Command.com', in certain parts of the test procedure. Although running XCOPY should hardly be cause for concern, this alert turned the overhead testing process into a very long, drawn out affair.

Due to the random nature of this warning, persistence eventually produced complete sets of test results for both the baseline condition (on-access scanner not loaded and the problem not evident) and the standard *ViruSweep* setting for 'continuous virus scanning' (check on file create and execute). With the overhead here turning up at a mere 7%, a sterling performance by any standards. [*Further checking reveals that the dubious alert mentioned here is attributable to the 'interrupt tracing' option of the behaviour monitor. This should be fixed or the default options changed. Ed.*]

As mentioned earlier, *eSafe Protect* was reviewed separately in the April issue of *Virus Bulletin* (see p.20). At that time, it was noted that its anti-vandalware component was incompatible with Turnpike, a popular UK mail and news front end. This problem still exists in the current version, the reason being that both programs use a custom WinSock as part of their Internet dial-up software configuration. Standard *Windows* Dial Up Networking proceeds as normal, but the inability to use *eSafe Protect* with other products that also install custom WinSocks could be problematic, especially since the anti-virus component of *ViruSweep* cannot be installed as a separate entity.

Conclusion

With marked similarities to the *eSafe Protect* product already reviewed, *ViruSweep* stands as better documented than its parent product. Speed is a strong point, especially on-access which operates with very little overhead. On the other hand detection of macro viruses is somewhat under par, a weakness which needs to be corrected if the detection rate is to be considered impressive.

Technical Details

Product: *ViruSweep Extra Strength.*

Developer: *Quarterdeck* USA, Tel +1 800 3543222, fax +1 813 5239700, email info@quarterdeck.com, WWW http://www.quarterdeck.com/.

Vendors: UK – Quarterdeck Corporation UK, Tel 00800 72127212, fax 00800 72127213, e-mail info@qdeck.co.uk., WWW http://www.quarterdeck.co.uk/. USA – *Quarterdeck Corporation*, Tel +1 813 5239700, fax +1 813 5232331, e-mail info@quarterdeck.com, WWW http://www.quarterdeck.com/.

Availability: This program requires a 486DX2-66 CPU, 8 MB of RAM, 12 MB of free hard disk space and a CD-ROM drive.

Version Evaluated: Version 1.0.

Price: UK £39.99; USA $69.95.

Hardware Used: 166 MHz Pentium-MMX workstations with 64 MB RAM, 4 GB hard disk, CD-ROM drive and 3.5-inch floppy drive running *Windows 95 (SP1)*. 233 MHz AMD K6 workstation with 64 MB RAM, 1.6 GB and 4.2 GB hard disks, a CD-ROM drive and 3.5-inch floppy drive, running *Windows 95*.

Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NW/199807/test_sets.html.

SUBSCRIPTION RATES

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

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

Editorial enquiries, subscription enquiries, orders and payments:

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

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

US subscriptions only:

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

Tel (781) 9377768, Fax (781) 9320251

END NOTES AND NEWS

The program for VB'98 – to be held at the Munich Park Hilton, Munich, Germany from 22–23 October 1998 – has been finalized. Delegates can move between technical and corporate streams, and a full exhibition is to run concurrently. Features of this year's event include a welcome drinks reception, gala dinner, partners program and speakers panel. Delegates who register before 31 July 1998 will receive a complimentary Leatherman tool. For a conference brochure and registration details contact Jo Peck; Tel +44 1235 555139, or email Joanne.Peck@virusbtn.com.

The developers of the content security product *MIMEsweeper* have recently conducted a survey among IT managers of 50 financial companies with over 100 email users. *Content Technologies Ltd* discovered that one quarter of the organizations do not have an access/content security policy in place. However, all the respondents who employ content security use the facility to detect email-borne viruses. Email info@mimesweeper.com for details.

Possible *Windows NT* security problems introduced by *Cheyenne Inoculan* and *Dr Solomon's Management Edition* were discussed on two *NT* security oriented mailing lists in early-to-mid June. Both problems revolve around the creation of potentially insecure shares on *NT* machines and the use of those shares in these products' software upgrade distribution mechanisms. *Inoculan v4.0* users not already running service pack 2 or later should download service pack 2A from http://www.cheyenne.com/CheyTech/Download/patches/techptch.html. Users of *Dr Solomon's Management Edition* are directed to the page at http:/www.drsolomon.com/products/avtknt/tnotes/ntbug.html, which explains the authentication and security processes built into the *Management Edition's* Update Agent.

E-Commerce and New Media: Managing Safety, Security and Malware Challenges Effectively is the title of the ***EICAR '99* conference from 28 February–2 March 1999 in Aalborg, Norway**. Abstracts must be submitted by 15 July 1998. Visit the conference web site http://www.eicar.com/ or send email to EICAR_Infosec@bigfoot.com for details.

Central Command Inc announces the release of the **on-line edition of the *AntiViral Toolkit Pro Virus Encyclopedia* (*AVPVE*)**, developed by Eugene Kaspersky of *Kaspersky Lab*, Russia. This comprehensive computer virus database contains thousands of virus descriptions and is frequently updated. An interesting aspect of *AVPVE* is the inclusion of demonstrations of various virus' activation routines. The encyclopedia is available free at http://www.avpve.com/.

***COSAC'98*, the 5th international conference on computer security, audit and control** takes place at the Slieve Donard Hotel, Newcastle, County Down, Northern Ireland, UK from 14–18 September 1998. Contact Helen Hawkins from *AKA Associates*; Tel +44 1232 738080 or email cosac@aka-associations.co.uk.

With the run-up to the official release of *Windows 98* on 25 July, several companies made big press releases to the effect that their anti-virus programs were *Windows 98* compatible. These are meaningless for the simple reason that any 'properly written' *Windows 95* product is, *ipso facto*, *Windows 98* compatible. It should be *hoped* that these anti-virus products were always *Windows 98* compatible!

Dr Solomon's will host a **live virus workshop from 14–15 July 1998 at the Barns Hotel, Bedfordshire, UK**. The intensive, hands-on course costs £695 +VAT. Contact Caroline Jordan for more information; Tel +44 1296 318881 or email Caroline.Jordan@drsolomon.com.

***Compusys Ltd* has joined *Norman Data Defense Systems (UK) Ltd* as a 'Security Partner',** distributing and selling the full range of *Norman* software in the UK and Ireland. *Compusys* will also bundle a copy of *Norman Virus Control* with every PC shipped. For more information contact *Compusys*; Tel +44 1296 505100, or *Norman Data Defense Systems*; Tel +44 1908 847410.

***Secure Computing Magazine's International Conference on Network Security* will be held from 2–3 September 1998** at the Mount Royal Hotel, London. Two optional workshops – Securing Unix Networks and Remote Access Security – are being run on 1 September. For information on prices and registration, contact Debbie Rosen at MIS; Tel +44 171 7798944.

Symantec* has announced the first step in integrating virus detection technology, recently licensed from *IBM, into its *Norton Anti-Virus* product range. *Symantec* sees this as a successful precursor to its eventual implementation of the immune system. This first update is available from http://www.symantec.com/.