June 1993 ISSN 0956-9979

VIRUS BULLETIN

THE AUTHORITATIVE INTERNATIONAL PUBLICATION
ON COMPUTER VIRUS PREVENTION,
RECOGNITION AND REMOVAL

CONTENTS

EDITORIAL

Mushrooms

This month's news of the widespread distribution of the Tremor virus (see p.3, 'The Virus Video?') will no doubt have caused one or two raised eyebrows within the industry. The virus has been relatively widespread in Germany for several months, and the event begs the question of how users and manufacturers can help prevent such accidents.

The first question is whether the software manufacturer was negligent - that is, were there adequate procedures in place to prevent such slip-ups occurring? That may be easily answered when considering a company which ships a Cascade-infected compiler, or a disk infected with the Form virus, but what about the more esoteric viruses? Unless computer users are happy to stick their heads in the corporate sand, this risk needs to be addressed. A good solution is not that difficult to find - if people are prepared to take the appropriate action.

The problems raised here can be addressed with three relatively easy steps: one for software distributors, one for users, and one for the anti-virus industry.

Firstly, software manufacturers should realise that the best defence against shipping infected software is clean computing practice. Virus scanners are*never* 100% reliable, and to depend entirely on this approach is foolhardy. It is far better to implement a good in-house security policy, and ensure that software is obtained from reliable sources. Like it or not, shareware can no longer be considered a reliable source, and should be avoided.

Secondly, users and distributors can obviate the requirement for their scanner to detect*every* virus known to man, by using integrity checking software. Even though checksummers are still not anything like as popular as virus scanners, they provide an unsurpassed line of defence against 'new' viruses. Integrity checkers will not stop a machine from being infected but do provide an early warning mechanism.

However, the real sin of of omission in this particular case has been committed by the anti-virus industry - specifically, the scanner manufacturers. The Tremor virus was first reported as being in the wild in the February edition of*Virus Bulletin*. Four months later, how many scanners can reliably detect the Tremor virus?

A quick survey of just a few members of the anti-virus community revealed the depressing truth: very few of the 'names' in the anti-virus industry actually detect it. As a straw poll, the first three virus scanners which came to hand were tested against the virus. The result? Neither*McAfee SCAN* v104, *Sophos Sweep* v2.49, nor *Dr Solomon's AVTK* v6.51 detect the Tremor virus.

The reason is very simple: the anti-virus industry is caught up in its own private 'numbers game'. The whole thing would be much more at home in a school playground. 'Ya boo - my package detects more viruses than yours', scream the opposing factions. Admittedly the rhetoric is couched in bland, politically correct terms, but the basic message (including the obligatory raspberry) is the same.

Manufacturers go to great lengths to make it appear that their product is 'top dog'. A recent survey commisioned by *S&S* from the so-called *'UKCVCC'* test centre, comparing 'latest' releases, found*Dr Solomon's AVTK* to be 99.9% effective. Given the antiquity of the competition (most of which, apart from Dr Solomon's, was several months out of date) this is hardly an earth-shattering conclusion. And what did the *UKCVCC* mean by 'latest'? 'The latest I had' was the reply. Had manufacturers been asked for the latest copies of their software? 'No.'

S&S is certainly not the only company to indulge in such practices - it is a fairly widespread and common way of selling one's product. However, all this simply acts to hide the true state of the industry.

The danger with playing the numbers game is that it is quicker to add ten simple file infectors to a scanner than one polymorphic virus like Tremor. Given that almost all scanner reviews simply test against a large number of viruses, a scanner compiled in this way will outperform its competitors. This means that there is a tendency for some of the more complex viruses to get swept under the carpet: reviewers generally only consider total numbers detected.

The industry reacted in a similar way tothe Mutation Engine. The code was circulated amongst researchers for several months without too much action being taken to ensure adequate detection. It was only when Vesselin Bontchev started publishing tests of products' detection accuracy that it became important. Until then, Joe User did not know that his scanner could not detect MtE, but once he did, MtE detection became a priority to vendors. All that matters is sales. As for users' hard disks - who cares?

Unfortunately this unhappy situation is unlikely to be brought to an end. If people want to produce scanners then they should place priority on keeping them up to date.The crux of the matter is that users are not aware of the shortcomings within the industry - and the industry certainly intends to keep them that way, lest it loses money. In the meantime, buyers are being treated in the exactly the way as mushrooms: they are kept in the dark and fed manure.

NEWS

Hackers Jailed

Two computer hackers have been jailed for six months for breaking into systems belonging to companies and institutions around the world.

Mr Neil Woods and Mr Karl Strickland were arrested along with Paul Bedworth (see *VB*, April 93, p.2), but unlike Bedworth, they pleaded guilty to the charges against them.

Passing sentence on the men, Judge Michael Harris said that he fully accepted that their hacking activities were not designed to damage systems, to misuse the information which they contained, or to make a profit from what they were doing.

However, he told them that the custodial sentences given were appropriate 'to penalise you for what you have done and for the losses caused, and to deter others who might be similarly tempted'.

This judgement, brought under the 1990 Computer Misuse Act, is a well deserved reward for all those who worked on the original case. Following the acquittal of Bedworth, many believed that a clear signal needed to be given to computer criminals within the UK that their activities would not be tolerated❑

The Virus Video?

An infected copy of *Pkunzip* has been sent out to subscribers of '*Channel Videodat*' in Germany. *Channel Videodat* is run by the German company *Videodat Medien*, which uses the 'spare' lines on a normal television broadcast to transmit computer software to subscribers - or in this case, the Tremor virus. The company claims that it has some 60,000 subscribers throughout Europe, and therefore the potential scale of the incident is large.

A user contacted the *Micro-BIT Virus Centre* in Germany on May 6th, reporting an infection of the Tremor virus, and claimed that the software had been downloaded by *Channel Videodat*. A sample was requested, and the infection was verified. The company was contacted, but they denied that they had sent out the infected software. It was at this point that *MVC* began to monitor the broadcasts.

On Friday 14th May, at 2pm, a Tremor-infected file was received - ironically in a copy of *Pkunzip* which was sent out together with *McAfee SCAN*. Two hours later, *Channel Videodat* discovered this error, and broadcast a clean version of the program.

Virus Prevalence Table - April 1993

Viruses reported to *VB* during April 1993.

Virus	Incidents	(%) Reports
Form	14	31.1%
Spanish Telecom	8	17.8%
Tequila	5	11.1%
Tremor	4	8.9%
Helloween	3	6.7%
Cascade	2	4.4%
New Zealand 2	2	4.4%
Eddie II	1	2.2%
Exebug	1	2.2%
Filler	1	2.2%
Halloween	1	2.2%
Italian-789	1	2.2%
Mosquito-Topo	1	2.2%
Nomenklatura	1	2.2%
Total	45	100.0%

Christoph Fischer, who has been instrumental in tracking down the source of the infection, said that the Tremor virus is extremely common in Germany, and that he has received many different reports of it 'in the wild'. Fischer went on to explain that it is unlikely that any action will be taken against *Channel Videodat* because the virus is not detected reliably by many scanners.

After this *faux pas*, *Channel Videodat* issued a somewhat fatuous press release, from which the following short extract is taken:

> 'With these events, CHANNEL VIDEODAT has demonstrated vividly the uniqueness of Data Broadcasting as a medium. Only the broadcasting medium CHANNEL VIDEODAT is in a position to distribute information, as well as practical assistance in the form of software, instantly throughout Europe. Only CHANNEL VIDEODAT is - as described in this case - in a position immediately, reliably and fully automatically to destroy virus infected programs and replace them with clean ones.'

What *Channel Videodat* fails to add in its press release is that it was also the only company in a position to cause such havoc in the first place!❑

IBM PC VIRUSES (UPDATE)

Updates and amendments to the *Virus Bulletin Table of Known IBM PC Viruses* as of 24th May 1993. 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 preferably a dedicated scanner which contains a user-updatable pattern library.

Type Codes

C = Infects COM files **E** = Infects EXE files **D** = Infects DOS Boot Sector (logical sector 0 on disk)

M = Infects Master Boot Sector (Track 0, Head 0, Sector 1) **N** = Not memory-resident

R = Memory-resident after infection **P** = Companion virus **L** = Link virus

Known Viruses

_125 (temporary name) - CN: A simple, 125 byte virus which does nothing but replicate.

```
_125            B41A CD21 1EBA 7701 B903 00B4 4ECD 2172 361F 1EBA 1E01 B802
```

_187 (temporary name) - CR: This virus is 187 bytes long, and like several other viruses which only have a temporary name based on their length, it does nothing but replicate.

```
_187            3D00 4B74 1480 FC77 7556 83C4 0858 1E57 8B36 B901 03F7 F3A4
```

_195 (temporary name) - CN: Another simple virus, 195 bytes in length.

```
_195            B43D B022 BAEC 0103 D6CD 218B D8B0 02E8 7500 80C4 01A3 0101
```

_212 (temporary name) - CR: A 212 byte virus which does nothing interesting.

```
_212            3D00 4B75 711E 0652 5751 5053 1E07 8BFA B900 01B0 2EF2 AE80
```

Abraxas - EN: A very primitive virus, which replaces the first EXE file it finds with a 1170 byte copy of itself. The only remarkable thing about this virus is that its author is known.

```
Abraxas         CD21 B43C 33C9 BA9E 00CD 21B7 4093 BA00 01B9 9204 CD21 C3B4
```

Arusiek - CER: An 817 byte virus. Awaiting analysis.

```
Arusiek         3DA9 4474 E450 5351 0656 5752 1E55 80FC 6C74 163D 004B 740F
```

Cascade.1704.H - CR: A very minor variant of the Cascade.1704 virus, where a few bytes have been changed in the payload part of the encrypted code. This variant is detected with the Cascade (1) pattern, but many anti-virus programs will not be able to distinguish it from other variants, unless they actually decrypt the virus first.

Chips - CN: This 877 byte virus is unremarkable, but it does present some problems to vendors - it is not possible to disinfect infected files, as the virus overwrites one byte in the file, without storing the original data.

```
Chips           B41A CD21 B911 00BB 5202 8037 6443 E2FA B419 CD21 A24D 02B4
```

CPXK - CN: An 1000 byte virus. Awaiting analysis.

```
CPXK            5BB4 3ECD 21E9 5FFF 8B44 3287 443A 8944 328B 4434 8744 3C89
```

Cysta.8045 - CER: A complex virus, 8045 bytes in length. It is probably of Polish origin, and seems designed to avoid certain anti-virus programs. Two smaller variants, 2711 and 2954 bytes are also known, but they are probably earlier versions. All three variants are able to infect SYS files in addition to regular COM and EXE files.

```
Cysta.2711      80FC 3D74 0880 FC4B 7403 EB04 90E8 0500 2EFF 2EC6 062E 8926
Cysta.2954      80FC 3D74 0880 FC4B 7403 EB04 90E8 0500 2EFF 2EB3 062E 8926
Cysta.8045      80FC 3D74 0880 FC4B 7403 EB04 90E8 0500 2EFF 2EB8 072E 8926
```

Experiment.416 - CN: This 416 byte virus is probably written by the same author as the other variant described in March.

```
Experiment.416  B41A CD21 B447 32D2 8DB6 7F01 CD21 B44E 8D96 1C01 33C9 CD21
```

Filename - CN: A 512 byte virus. Awaiting analysis.

```
Filename        B41A CD21 B902 00BA E802 1E0E 1FB4 4ECD 211F 3C00 7403 E93E
```

Fisher.2420 - CER: This is an advanced, fully stealth virus, which has not been fully analysed, but does not appear to be designed to do any damage. It is 2420 bytes long and contains the text '(c) Copyright 1991-92 by Fisher. Version 2.0'

```
Fisher.2420     7431 80FC 5674 2C80 FC41 742A 3D02 CC74 03EB 0590 B8CC 4BCF
```

Hallo - CN: The name of this 496 byte virus is derived from the message 'Hallo! I have got a virus for you!' which it may display.

```
Hallo           B900 00BA 0000 8B9C CC02 B002 B442 CD21 7303 E9C3 0089 84CA
```

Harm - ER: A 1082 byte virus. Awaiting analysis.

```
Harm            3DFE 4974 3BB9 F100 2E89 0C3D BC4A 7430 B913 012E 894C 023D
```

Intrep.1092 - CEN: A 1092 byte virus. Awaiting analysis.

```
Intrep.1092     F7F1 83FA 0074 14B9 1000 2BCA 8BE9 01AD 5E04 8395 6004 0040
```

Leprosy.Crawler - EN: This 562 byte virus overwrites EXE files, but like other overwriting viruses it is extremely unlikely to spread.

```
Leprosy.Crawler 7F09 80FA 0074 EB88 1603 01C6 06E0 0100 C606 E101 04C6 06EA
```

Lyceum.1888 - CER: This Russian (?) virus contains a long, encrypted message about an institution named MIREA (Moscow Institute of Radioengineering, Electronics and Automation)

```
Lyceum.1888     FB3D CDAB 74F3 2E80 3E40 07FF 74E4 80FC 4E74 0580 FC4F 7525
```

Mr. G - CN: A simple, 253 byte virus which contains the text 'Mr. G' at the end.

```
Mr. G           80A8 E901 63E2 F7BA EA01 03D6 B44E 33C9 CD21 B905 008B D980
```

Mx - ER: This 335 byte virus does nothing but replicate.

```
Mx              3D00 4B75 4A50 1E52 0653 33C0 8EC0 26A1 6C04 2503 003D 0300
```

November 17th.855.B - CER: Only slightly different from the original variant, and detected with the same pattern.

Over.4032 - EN: A primitive, overwriting virus, written in Pascal. As with other high level language viruses, the search pattern should be used with care, because of the risk of false positives.

```
Over.4032       9827 9A46 0298 2789 EC5D C204 0005 2A2E 6578 6503 4D5A C055
```

Porridge - CN: This 1384 byte virus sets the 'hidden' attribute of all the files it infects, but has not been fully analysed. It is probably of Russian origin.

```
Porridge        50FF 2605 0158 B43D 5ACD 21A3 2B01 5072 05B8 FFFF EB02 33C0
```

Radyum - CR: Two variants of this virus are known, 448 and 519 bytes in length. They are encrypted, and the search patterns below should be used with care, as there is a chance of false positives.

```
Radyum.448      BB?? ??B9 D800 8137 ???? 83C3 02E2 F790
Radyum.519      BB?? ??B9 FB00 8137 ???? 83C3 02E2 F790
```

Silly Ice - CN: Three viruses, which were written by members of the ARCV group, but are listed as a separate group as they are quite different from all the other ARCV viruses. The three variants have infective lengths off 159, 199 and 224 bytes. The 224 byte variant is flawed, and disinfecting infected files may be impossible.

```
Silly Ice.159   48E8 5900 3E89 8601 012D 0300 8945 FEB4 40B9 9F00 8D96 0001
Silly Ice.199   4848 4889 45FC 33C9 E866 00B8 023D E863 0089 45FE B43F 8D55
Silly Ice.224   33C9 E87D 00B8 023D 8D94 0402 CD21 8984 E401 87DA E890 00BA
```

Storm.1163 - CR: This variant is 10 bytes longer than the variant reported earlier, but very similar and detected with the same pattern.

Timid.431 - CEN: Yet another 'buggy' member of the Timid family. It is detected with the Timid.306 pattern.

Tver - CR: A 308 byte virus which does nothing but replicate. As Tver uses instructions which only exist on '286 machines and above, infected programs may crash on XTs and other 8088 and 8086 systems.

```
Tver            601E 0616 9C3D 004B 7403 E981 00B4 3DB0 02CD 2173 03EB 7790
```

V-160 - CR: This East European virus is among the smaller resident viruses, and as should be expected, it does nothing but replicate.

```
V-160           80FC 4B75 54FE C074 E1FE C875 4C60 1EB8 023D CDE7 7241 8BD8
```

VCL.384 - CN: Detected with the generic VCL-1 or VCL-2 patterns.

VCL.394 - CN: A simple overwriting virus. This pattern should be used with care, as it will detect most unencrypted VCL variants.

```
VCL.394         B41A 8D56 80CD 21B4 4EB9 2700 5ACD 2172 09E8 1400 7304 B44F
```

INSIGHT

Doing IT the *Digital* Way

Computer security is at the forefront of most large corporates' minds - as computer hacking becomes increasingly common, and with more and more confidential data being stored on company machines, they cannot afford any other attitude. Tony Pitt is a member of the team responsible for computer security within *Digital*, and has recently been involved in the Paul Bedworth hacking trial.

Pitt's entrance into the world of computer security was purely by coincidence. 'I got into it by accident really', he laughed, 'I happened to be around when a security problem with VMS was reported. I was the person to take the next call and worked on it at length with a colleague. I made some contacts within *Digital*, and when the next security problem came in, they had my name, so I was given that call. From then on, I was the person doing security!'

The Bedworth Case

Pitt was recently in the public eye as a witness at the trial of Paul Bedworth at Southwark Crown Court. How did he get involved? 'Basically, I started handling reports from our customers on Bedworth's activities in the UK around Easter 1989. Gradually from then onwards I got more involved both with the Police and *British Telecom* as the investigations concentrated on the three individuals. Some of those victims had simply found someone knocking at the door - and the system refused to let them in. Those are the good ones. The bad ones were situations where systems had been hacked.'

'There was one case where I went in and advised the company on what to do. They did *almost* everything that I said, and a few months later they 'phoned me up and said "We've been hacked again". They showed me the list and there were a few vital steps missing. We had to do the whole thing again. It's tragic.'

Bad Management

It is difficult to understand how three young hackers could gain access to so many different computer systems. Are mainframes inherently that insecure? 'Not really. In every case, they got their initial access as the result of bad passwords. Back in '89 there were still lots of cases of usernames and passwords like "System Manager" or "Field Service". Those have all gone now, but still password management is poor. The facilities within VMS are better now than they were - that helps. But it is still down to the users to choose good passwords. Actually I've never liked the word password. Perhaps if they had called it a "passphrase" people would have picked better passphrases from the start, rather than simple dictionary words, which are easy to crack.'

Pitt: 'The biggest defence against computer viruses is clean computing practices'

'On one particular system that I looked at, they were concerned about the security of their passwords. In a matter of a few hours, on a machine back in the office, I had cracked 75% of their passwords - including the IT Director's. I don't think we ever told him that!'

'Once they had got past the initial entry into the machine, they just poked around until they found a way of gaining privilege. Sometimes through cracking the passwords on other accounts, in other cases through poor system management. Generally, they simply set themselves up so that they could use that system as a jumping off point to make calls to other systems. The principal damage in many cases was telecom bills. We have seen incidences of telecom bills of tens of thousands of pounds run up in the space of a few weeks. Nobody likes those when they arrive.'

Not Guilty

Pitt was present when the jury returned its not guilty verdict on Bedworth. Was he surprised? 'Yes. I don't think anybody was confident that he was going to be found guilty on all charges, and nobody had any good ideas as to what he would be sentenced to as a result. I think everybody was surprised that he was acquitted of everything - there was no argument about the material evidence. His barrister admitted the unauthorised access, admitted the use of other people's telecom accounts and so on, and so we are left to guess as to why he was actually acquitted. I have my theory...' What is Pitt's theory? Pitt smiles, but refuses to elaborate.

Many of the computer law pundits observing the case heralded the result as the demise of the Computer Misuse Act. Pitt disagrees. 'My own feelings were that the charges

brought were inappropriate, and as straight CMA charges under section 1 and 3 there would have been no problem. The Police and the Crown Prosecution Service will have to be much more careful about the charges next time. The thing which seems to be called into question is the use of a conspiracy charge in order to deal with a group of individuals - and that is where I believe that the case fell down.'

The Computer Misuse Act does not contain anything to cover reckless actions against a computer. Is this a shortfall? 'There is no doubt that what all three defendants did in several cases was extremely reckless - they did not know the extent of their actions. The most quoted case was for the European Organisation for the Research and Treatment of Cancer, where the surgeons treating cancer patients were unable to access vital information - that was as a direct result of the hackers' activities. It wasn't their intention to do that, but they were reckless in their actions - and they can't be charged for that specifically.'

Pitt believes that because of the way computers affect everyone's life, users have a responsibility not to misuse them.'Maybe computers should be covered by such a clause because everybody's safety depends on it all the time. Take the example of flight. I don't know if those hackers went anywhere near systems involved in air-traffic control - they probably don't know if they did! In those circumstances it probably makes sense to include this type of clause.'

The Human Factor

Hackers like Bedworth seem to be able to get in to a wide variety of systems. Can it be that difficult to lock them out? 'Security in all areas is much more than just technology - I would tend to say that it is twenty per cent technology and eighty per cent management. The technology provides some of the features to control what is going on, but a lot of the rest is management of the users - how they choose passwords for example - and what procedures there are about how they use computers. That balance is probably more in favour of management when you talk about PCs.'

Has Pitt's role been affected by the rising numbers of computer viruses? 'Yes, in the past I have been very much involved in hacking issues, but PCs are getting more important. More reports of viruses are coming in, and I have to follow those up and do whatever is necessary. I much prefer to get involved before they start causing actual problems - to get people doing the right things to start with. In effect, to stop them at the door.'

'The biggest defence against computer viruses has got to be clean computing practice - not transferring floppies around, not running software of unknown origin. Anyone who avoids those two things completely doesn't need virus scanners or anything like that. In practice, of course, most of us are in a position where we have to exchange material between machines, and under those circumstances, scanners provide the technology as part of that complete solution.'

How does *Digital* try to prevent introducing viruses in to its system? 'I wouldn't want to go into the details of policy, because it's policy not to. Basically though, we rely on what we have just described: not running unknown software and not exchanging diskettes unless really necessary.'

Which viruses has Pitt come across?'The standard ones. Probably more interesting is*where* we have come across them. We appeared to have a case of a virus on a distribution kit, which was very strange, since the kit had been produced from a scanned master from a disk copying machine. That was a false positive report. Much more seriously, a number of PCs hired from a third party were brought in. As is standard, they were scanned before use, and were found to be infected. The third party - whose business was to hire PCs - had no anti-virus procedures in place.' Surely this must have happened a long time ago? 'Not as long ago as it ought to have been! That was within the last two years. On querying this their attitude was almost ''So what?'' '

The biggest problems arise for Pitt when scanners produce false alarms. 'I think that we've still got a fight on with users who view a PC much like they view a terminal on their desk. They switch it on in the morning, do their work, and switch if off at night. Why do they have to do scanning for viruses? When those users come up with false positives, we then have the even bigger job of explaining why the scanner told a lie. Why do they have to bother with this effort if they can't trust the result anyway? That's a very difficult problem. I don't think that there is an answer to it at the moment.'

Predictions

What about the future? 'I don't know. I think it is too dangerous to look into the future. I suppose we have to hope for the day when we make a breakthrough somewhere that puts paid to viruses being introduced as they are at the moment. One positive step in that direction is when*Windows NT* comes along. At least those users have a way of adding system security in a way which isn't available under MSDOS. That will make it very much more difficult for viruses to spread. However, because the security is optional then it isn't clear whether they will use it.'

'Clearly as the number of viruses goes up, the time taken to analyse them and add them to scanners goes up, and eventually we will reach a point where it simply isn't reasonable to scan for viruses as we do at the moment. I suppose we could hope that the individuals who write viruses will go away, but I don't see that happening.'

VIRUS ANALYSIS 1

Eugene Kaspersky

Cruncher - The First Beneficial Virus?

The first time I ever heard about the dispute over whether there could ever be such a thing as a useful virus was many years ago, when I was analysing the first virus I had ever seen. One of the articles which I read at the time was about the definition of a computer virus and the philosophical aspects of viruses. The article went on to discuss what the future might hold, and whether or not one could ever have a useful virus.

At the time, I was not ready to take a firm standing point on this issue - in fact, I'm still not ready to decide. For example, a well-written boot sector virus which looked for lost clusters could arguably be useful. Once you begin to consider the beneficial things a virus could do, the list is rather long. There is a multitude of small 'housekeeping' tasks which a virus could perform, all of which could be inserted into the virus' algorithm.

I hope that this does not appear to be propaganda for the legitimacy of virus writing. Computer viruses bring immense problems with them, and seriously compromise the security of machines. However, life brings a lot of surprises, and to become fixed with one particular viewpoint is always a bad idea - one of these surprises was that the Earth is not flat, but round as a ball. In the 15th Century, who would have thought it!

However, regardless of all of the above, the question remains - can we have a useful virus? If we can, then the Cruncher virus could well be it.

The Virus Which Saves Your Disk Space

This virus takes its name from an internal text string 'Cruncher V1.0ß' which is inserted into the end of the virus body. This word has a special meaning in the world of file compression - 'crunching' is the name of one of the file-packing methods used by most popular data compressors.

On the face of it, Cruncher looks like an ordinary memory-resident parasitic COM-file infector. It hooks Int 21h when it is executed and then alters the Memory Control Block list, leaving itself neatly installed in high memory.

When Cruncher is memory-resident, it infects on the DOS Load and Execute function. During the infection process, the virus intercepts Int 24h (the DOS Critical Error Handler) to ensure that spurious error messages are not displayed. The virus does not alter the time and date stamp of infected files, nor their attributes.

So far, Cruncher appears to be almost an ANSI-standard file infector virus, but unfortunately things are not nearly as simple as this first analysis would show. The additional code in the virus makes up a complete data compression routine. The Cruncher virus compresses the body of the host file when it infects it - so a hard disk thoroughly infected by this virus will have more space on it than before the infection - with no resulting loss of data!

The Origin

The virus contains the text string '[MK / Trident]'. This message is present in several of the more complex hacker products, including the four versions of the TPE - the Trident Polymorphic Engine, which is rather like the MtE.

This means that virus writers can append that OBJ module to their viruses to make them polymorphic and difficult to detect. About six TPE-based viruses are known at this time, including the Girafe virus and the last version of the Coffeeshop and Civil War viruses.

The 'MK' label is present in several other viruses which are comparatively advanced - these are the MtE-based version of the Coffeeshop virus and WinVir-1.4, which is capable of infecting *Windows* executables.

Resident Operation

When the virus is memory-resident, it intercepts the main DOS interrupt Int 21h and checks function 4B00h (Load and Execute) and function 33E0h which is used by the virus as an 'Are you there?' call.

When a Load and Execute (AX=4B00h) function is trapped, the virus checks the file's name and extension. Version one of the virus only infects COM files, although it excludes any files which have the first letters CO. Version two of the Cruncher virus infects both COM and EXE files, but excludes files which begin with the letters SC, CL, VS, NE, HT, TB, VI, FI, GI, RA, FE, MT, BR, or IM.

The virus opens the file and examines five bytes of its header to ensure that the file is not already infected. If the target file length is less than 256 bytes or above 61440 bytes, the virus will not infect it.

Slimming Down

If the file is deemed suitable for infection, the virus reads the whole file contents into one of two temporary segments (128k) of system memory. The virus then infects the file *in*

memory, by appending the virus code and adding a jump instruction at the start of the host file.

Up to this point, the virus has acted like any other file infector - however, the virus now starts to pack the infected memory image of the file using the same algorithm as the DIET utility. This compression is used over the entire file, i.e. the host and the virus body.

The infection routine ends here, and the compressed file is copied back to disk. The virus closes the file, restores the file attributes and time/data stamp and releases the temporarily allocated segment of system memory which was used during infection. The result of this is that the virus code is now stored within the file compression - and therefore not immediately visible. The compressed file is completely DIET-compatible to the extent that it is possible to use the DIET utility to decompress the executable!

Unpacking and Installation

When an infected file is executed, the file begins to unpack itself, using the DIET algorithm. When the unpacking routine is complete, the virus installation code is executed. This checks the system memory to see whether the virus is already resident by using an 'Are you there?' call. If it is not, the interrupt handlers are hooked into place and the virus becomes memory-resident.

Detection Problems

Reliable detection of the Cruncher virus is a very difficult task because the actual virus code is hidden within the compressed file. In this case it is not acceptable to search for the decompression routine (effectively, the decryption routine) because that code has a perfectly legitimate role in other programs. It is also not possible to use a Hex pattern search (even with wildcards) as the contents of the compressed file will depend on the contents of the host file.

When a file is compressed using DIET, an algorithm developed by Lempel and Ziv is used. The compression is based on creating a dictionary of 'words' which make up the majority of the file. Compression of this type is known as 'adapted word compression', which can be thought of as creating 'abbreviations' for longer expressions - just as one abbreviates Terminate Stay Resident to TSR.

For example, by using this method the string '111122231111' will be compressed to '11 [repeat 2 bytes from offset 0] 2223 [repeat 4 bytes from offset 0]'.

The contents of a file are therefore packed as the sequence of new words and pointers to words which have already occurred in that file.

This means that the byte sequences contained in the compressed file will depend not only on the contents of the virus code but also on the contents of the host file. Therefore the contents of the compressed infected file will differ vastly for different host files.

This presents rather serious problems when considering how to detect the Cruncher virus. I can see no way of detecting every single infection of the virus unless the entire file is unDIETed [*Fattened? Ed.*], and then scanned. However, this process is both time and resource consuming - if the target disk contained a number of legitimate DIETed files, the scan time for the disk could be unacceptably high.

It is probably possible to search for the strings '[MK / Trident]' and 'Cruncher V1.0ß'. Although these are nominally compressed, the brief experiments which I have conducted show that infected files are detected in 75% of cases - which is enough to raise the alarm, but not nearly enough for reliable detection.

CRUNCHER

Aliases:	Cruncher-2092, Cruncher-4000
Type:	Memory-Resident, Appending Parasitic, Polymorphic
Infection:	COM files only (Cruncher-2092) COM and EXE files (Cruncher-4000)
Self-Recognition:	
Files	Checks contents of first five bytes
Memory	'Are you there?' call using INT 21h with AX=33E0h.

Hex Pattern:	No simple search pattern is possible. Many infected files contain 'corrupted' incidences of the following strings
	Cruncher-2092:
	`[ MK / Trident ] Cruncher V1.0ß`
	Cruncher-4000:
	`*** CRUNCHER V2.0*** Automatic file compression utility`

Trigger:	None
Removal:	File disinfection is possible but difficult. Under clean system conditions identify and replace infected files.

VIRUS ANALYSIS 2

Jim Bates

Form II - Stirring Up Trouble

A major problem in anti-virus research is highlighted by the continuing activities of an irresponsible and malicious minority who have a slight knowledge of computers and decide to exercise their minds by modifying an existing virus into a new variation. This is particularly reprehensible when the people concerned are currently undergoing some form of computer training in a university or college.

It seems self-evident to me that anyone who does this has demonstrated his complete lack of concern for other computer users and thereby disqualified himself from any further involvement in computing. The fact that some companies are prepared to employ known virus writers simply indicates their own unscrupulous attitudes and compounds the problem. Such companies should be denounced and ostracised until they are prepared to recognise and assist in controlling this menace.

One such 'new' virus variation has recently been reported at large in a UK university and while it is not yet clear whether this is where the virus originated, the police have been informed and investigations are well under way.

Description

The new variation has been called Stir by its author (inserted at the end of the code) but since it is a close equivalent to the Form virus, a better name is probably Form II. The modifications introduced to the original virus consist of simple juxtaposition of some code instructions and the addition of a different trigger routine. The general functionality of the virus has not been changed and this means that the risk of data destruction remains similar to that with Form.

Just like the original Form virus, Form IIis a boot sector virus which infects the DOS boot sector of fixed disks and the boot sector of floppy disks. The original (i.e. uninfected) boot sector is stored in the final sectors of fixed disks and this is one of the features which will irreparably destroy any data stored there.

Installation

Form II is 1024 bytes long and becomes resident and active when an attempt is made to boot from an infected floppy disk. The common method used by most boot sector viruses of installing code at the top of memory is exploited here and the virus then hooks the disk services interrupt via Int 13h. The system date is then checked for an impossible value - this may be deliberate but is more likely to be a mistake on the part of the virus writer.

However, as the code is written, the check fails and the virus then hooks the DOS Critical Error handling service Int 24h. This is the service that produces such messages as 'Abort, Retry, Ignore or Fail?' when an error occurs which requires user intervention. Once this hook is installed, the code continues with the normal boot process leaving the virus code resident and active at the top of memory.

Operation

The resident activity of this virus centres around the interception of the Int 13h interrupt vector. Apart from the swapping of some instructions in the primary section of this intercept, this code is identical to that in the Form virus. Thus it intercepts only requests to read the boot track of a floppy disk and holds the request while the target floppy is checked and infected, before calling the original Int 13h handler.

Infection

Fixed disk infection occurs during the original installation code execution (i.e. when attempting to boot from an infected floppy). This consists of collecting the active Partition Boot Record and checking it for infection by examining whether the word at offset 3Fh is 01FEh.

"the police have been informed [about the virus] and investigations are well under way"

A check is also made to ensure that the disk is configured with 512 byte sectors (infection aborts for disks configured differently). If the disk is not already infected, the contents of the original DOS boot sector are written to the last sector on the disk (as reported by a previous call to obtain the global disk parameters). Then the second sector of the virus code is written to the penultimate sector of the disk. No check is made prior to these writes to see whether the target sectors contain data. Thus it is quite possible for this virus to destroy data on the partition which uses these sectors even though that might appear as a different drive to DOS.

For example, a drive with two partitions would contain the first sector of the virus code on the PBS of the first partition and the remainder of the virus together with the original

PBS, on the second partition. In this case any destroyed data would be on drive D.

It should also be noted that the virus makes no attempt to protect the sectors that it uses; if the sectors were unallocated, DOS would eventually overwrite them with data. If they were allocated then they might eventually be modified by the parent program. In either case, the results would be unpredictable and possibly disastrous as the machine would attempt to boot using garbage code.

When infecting floppy disks, the virus is a little more considerate. The File Allocation Table is searched for unallocated space and if any is found it is used by the virus and marked as bad in the FAT. It is interesting to note that if there is no space available on the target disk then the virus does not infect it.

Trigger

This is where the virus differs from its original ancestor. In the original Form virus, a routine was hooked whenever the system date was set to the 18th of the month and caused keyboard clicks. In this variant, the routine is not date-dependent (see the reference to date checking in the Installation section) and is active whenever the virus is memory-resident.

The trigger routine is hooked as an intercept of the DOS Critical Error handling service and is invoked whenever such an error occurs. It begins by scanning the screen and counting how many characters are displayed. If there are fewer than 768 characters on the screen, the routine exits without taking any action.

If the trigger conditions are met, a simple looping routine is invoked which has the effect of making each character in turn (starting at the top left of the screen) fall down to the bottom and disappear. Any character at row one, column one is ignored.

The process is extremely primitive and will take several minutes to complete, during which the machine cannot be used. Once all the characters on the screen have been cleared in this way, control is passed back to the system.

Under certain circumstances the screen may then reappear as it was before the virus triggered and processing can continue normally. However, there are occasions when the screen is not rebuilt correctly and the resulting confusion for the operator could cause inadvertent data damage.

This virus has no encryption code and no stealth capability and should therefore be easily detectable by existing generic anti-virus software and by scanners looking for specific viruses once they have been updated.

Conclusions

The main point worthy of consideration when viruses are 'manufactured' in this way is exactly the same as for any computer viruses: the blatant disregard for other people's property. Doubly galling is that the virus author does not have the ability to understand fully what he is responsible for destroying, and is carrying out his 'computer vandalism' in a 'second hand' way.

When such activity emanates from within a place of training and education (which may well be the case in this instance), it is doubly disturbing and the authorities involved have a duty to identify and expel the person responsible or risk their organisation being branded as a source of unethical, irresponsible and potentially criminal behaviour.

FORM II

Aliases:	STIR
Type:	Memory-resident, DOS boot sector.
Infection:	DOS boot sector of fixed disks and boot sector of floppy disks.
Self-Recognition:	
Disks	Checks whether the word at offset 3Fh in the DOS boot sector is 01FEh.
Memory	None

Hex Pattern:	The following pattern will be found in the DOS Boot Sector
	`E82F 00E8 4100 BF46 03BE 4100`
	`BB4C 00E8 00C7 B404 CD1A 80FA`

Intercepts:	Int 13h for infection of floppy disks. Int 24h for Trigger routine.
Trigger:	Clears a text screen by removing one character at a time
Damage:	Any data stored in the last two physical sectors of a fixed disk will be overwritten. If this area is subsequently modified it may become impossible to boot the machine properly.
Removal:	Specific and generic disinfection is possible. Use command SYS [drive name] to remove from systems running DOS 3.x and above

FEATURE

Dr Luca Remotti
ISTEV

The Italian Job

The major challenge when attempting to study computer crime scientifically is the collection of statistics. Many organisations are unwilling to comment on computer crime, and this is particularly true in Italy.

The Italian *Ministry of Justice*, investigating revision of the criminal code to include legislation on computer crime commisioned *ISTEV* (*Istituto per lo Studio della vulnerabilità della Società Tecnologicamente Evolute*[1]) to carry out a study of information system abuse.

The research was based on a survey aimed at bodies with structural or organisational features which particularly expose them to information systems abuse. The panel was made up of 80 subjects from different areas, including banking, high-technology industry, telecommunications, and public administration.

The objective of the survey was to obtain an overview of:

- IT risk awareness of the main organisations producing goods and services and of the bodies of public administration.
- The organisational, logical and physical protection methods which have been implemented.
- The registered cases of systems abuse, the damage suffered and the countermeasures implemented.
- The means of verification of the software adopted and the cases of virus infection.
- The perception of insiders of the need to regulate the subject through a revision of the Italian penal code.

The Structure of the Survey Panel

The information and the evaluations provided by surveyed subjects covered in the most representative way those sectors particularly exposed to Information Systems abuse. The survey bodies were: 32.5% Manufacturing Industry, 20% Services Provisions, 35% Banking, Finance and Insurance, and 12.5% Public Administration.

[1] *Institute for the Study of vulnerabilities of Technically Developed Societies*

The panel was made of medium and large companies and organisations, and was classified according to their number of employees: 25% of the organisations have more than 200 employees, and 65% over 1000 employees.

73% of the interviewed parties declared a high degree of dependence and 21% a medium degree of independence of the organisation on Information Systems.

The dependence of operations on information systems is determined by the level of automation of the core business and the possibility of activating backup procedures immediately.

The Awareness of the Risk

Nearly all subjects (97.5%) agreed on the existence of a risk of Information Systems abuse. Over 60% of the subjects thought the risk to be tangible as well as intangible.

Furthermore, 71% of those interviewed indicated that the continuity of their operations was the most critical factor, and over 50% were aware of the fact that the organisation's image could be damaged; threats to data, information and goods were lower in ranking.

The Means of Protection

Over 65% of the participants in the survey felt that the Information Systems protection level of the organisations was adequate. 30% found it wanting, and 4% that it was totally insufficient.

The main means of protection implemented were the physical protection of the site and access control to data and software - these were used in approximately 80% of the organisations. Neither distribution of critical functions nor encryption seem to be widely used.

Only 50% of the organisations claimed to have set up an independent unit managing Information Systems security. This fact shows how the awareness of risk to Information Systems does not necessarily involve the implementation of a means of organisational protection.

Less than 50% of the organisations investigated are insured against Information Systems abuse: of these, nearly 80% have insured the hardware, 59% the software and only 22% the continuity of operations.

Incidence of Abuse

Of the organisations surveyed, 20% declared to have suffered from Information Systems security breaches, revealing some 41 cases of abuse.

The abuses indicated were:

- Computer Fraud 45%
- ATM Fraud 17.5%
- Computer Deception 10%
- Damage to Data or Software 10%
- Computer Espionage 7.5%
- Unauthorised Software Copying 5%
- Unauthorised Access to Computers 2.5%
- Unauthorised use of Information Systems 2.5%

In all cases but one it had been possible to reconstruct all the phases of the criminal action and about one third of the perpetrators have been identified. It was specified that in some cases it has not been possible to prosecute the identified offender because of lack of legislation.

The objects of the abuse have been, in order of frequency: data, CPU time, software, the telecommunications system and terminals.

Different sanctions were applied against the malefactor: in one case the person was replaced, in seven cases the person was dismissed, and a damage claim submitted. In twenty-one cases the offenders were prosecuted under Italian law.

Six of the organisations did not apply any sanction because of the difficulty of the collection of evidence and the lack of any relevant criminal legislation.

''The survey pointed out that most tests are made on mainframe software - what happens on PCs seems to be generally neglected''

In 50% of the cases of abuse the organisations suffered from damage involving: in four cases loss of goods, in seven, unauthorised access of data or software and in three cases unauthorised manipulation of software or data.

The countermeasures implemented involved purchasing new hardware and software means of control and reviews of organisational control procedures.

Viruses

65% of the organisations have implemented software testing, and 70% of these found infected PCs or networks. Remarkably, the virus phenomenon is considered separately from the cases of information system abuse. The survey pointed out that most tests are made on mainframe software - what happens on PCs seems to be generally neglected. No tests are done on software installed by users, or modified by users, are performed. This is the cause of the high occurrence of viruses on PCs. In most cases of infection, the infection ocurred through disks coming into the system.

In addition, no organisation pointed out the direct or indirect costs of virus detection, data loss and recovery and operations interruption. The views on viruses were contradictory: 70% of the organisations interviewed indicated that interruptions of operations was a critical Information Systems risk, yet the same organisations did not seem to take into account interruptions due to virus infection and recovery.

Anywhere, effective fighting of virus infections cannot be based on technical means (anti-virus software) but must rely on an Information Systems Security Culture, which must be spread among users to raise awareness of the operational and economic need for Information Systems and data integrity.

The Italian Legislation

Nearly 80% of the organisations felt that the Italian criminal and civil legislation on Information system abuse was inadequate. According to 70% of those interviewed, unauthorised data or software modification should be considered a criminal offence; 60% wished damage and unauthorised access to data to be included in the penal code. 50% of those interviewed wanted unauthorised use of data and of computing time to be considered a criminal offence.

Furthermore, 80% of the organisations were in favour of an institution which could act as an observer in the field, monitoring technical, economic, organisational and judicial aspects of the phenomenon in order to deliver real-time information to users about the current threat to computer systems. The organisations which were in favour of such a body cited the requirement that it should provide reliable information through trusted bodies.

Conclusions

The analysis summarised above leads to the conclusion that the incidence of Information System abuse in Italy is growing, just as it is throughout the industrialised countries. It is estimated that there are about 4,300 cases of computer crime in Italy every year.

The awareness of insiders on the matter is high, but there is a lack of overall comprehension of the problem and a failure to implement adequate means of protection. The contradictory views concerning computer viruses was worrying, and it is hoped that education will help the situation.

✉ LETTERS

Dear Sir,

I refer to your editorial in the March issue entitled 'Law and Disorder'.

While a different outcome of the trial in question might have been desirable, your editorial puts forward some rather disturbing views in a general context. It draws an analogy between housebreaking and hacking. There is indeed the offence of 'breaking and entering', but if you leave your door open, someone cannot be prosecuted for entering your house. To use your own words, why should a computer system be any different?

There are close parallels between leaving doors open (or the keys in them) and using default passwords (or other such sloppy practices). Your suggestion that it is not a system manager's fault if the system is hacked is actually a ludicrous notion. If you entrusted your money to a bank which left the keys in its safe door and the money was stolen, I am sure you would expect them to bear the loss rather than you; in other words you would hold them responsible. If you habitually left your keys in the house door, or made it out of papier mache, I doubt your insurance company would stand for many (if any) claims under your theft policy; they expect you to take due precautions.

This reflects current society as a whole. Normal citizens accept the need for crime prevention, and we spend a lot of money and public energy on it; similarly, motor manufacturers are investing like never before in making cars harder to steal. Why should IT managers not live up to the same facts of life?

Given the volume of advice that has been offered by the likes of your goodselves for so long, anyone foolish enough to leave default passwords in place shows a degree of negligence which should be judged as highly culpable. If personal data were involved, I would hope that such folly could be considered as a breach of the Data Protection Act.

The view you put forward encourages the negligent IT manager to hope that the state will protect him by martyring hackers with far greater penalties than it exacts from transgressors of other laws.

You also attach much importance to the value of the damage, but the law is as much, if not more, concerned about the intent of the transgressor. Apart from that, few 'normal' offences seem to be rewarded by penalties which are commensurate with damage caused, even when there is intent. Computer systems are far more complicated, for example because values are hard to prove, and 'contributory negligence' must be a minefield.

People in the IT industry who expect to be afforded much more 'special treatment', and to get a lot of sympathy, should think again. The public at large does not have much sympathy with computer systems, and can we realistically expect them to? Can IT professionals expect to be given priority when society is struggling with enough other problems, and when they have so many of the answers in their own hands?

Don't get me wrong; I would love to live in a world in which we could leave our doors on the latch, and did not have to invest heavily in protecting every aspect of our daily lives. I am however a realist, and an erstwhile IT manager and 'consultant' who thinks that IT managers should take their responsibilities far more seriously than many do. Indeed it is they who do little for the image of the industry; if the public cannot have faith in IT systems and those who manage them, we will all be the losers.

Yours sincerely,

A F Leader
Consultant.

[*Mr Leader is well justified in his view that System Managers should be held responsible for security breaches. The point I intended to make was that this is immaterial when considering the magnitude of the accused's crimes. As for Mr Leader's thoughts on penalties commensurate with the damage caused, I firmly believe that the recently granted custodial sentences are apt rewards for the hackers' efforts. Ed.*]

Dear Richard,

The feature in the April 1993 issue of *Virus Bulletin,* 'Using Security Modelling to Combat viruses' by Mr Winn Schwartau, is one of the more nonsensical articles I have ever read in your excellent magazine. Not that Mr Schwartau does not understand his business. Anybody in computer security will confirm that the techniques he advocates do indeed perform most of what he claims. In our company, *Computer Security Engineers Ltd,* we have 12 criteria instead of Mr Schwartau's seven, but we adhere to the same basic philosophies.

From the contents of his article, it is thus my conclusion that Mr Schwartau is just not in the anti-virus business, because he commits two serious and fundamental errors in his reasoning when it comes to dealing with vira, making his conclusions completely false.

The first one is believing that his reference monitor will report the truth to him and in actual fact be an impartial mediator. Mr Schwartau believes in the integrity of his software methods. Anybody in the anti-virus industry will tell him that this is old fashioned naïvety. Mr Schwartau's method will not protect against malicious intent, although it will protect against common accidents. Thus, from a technical point of view, this method does not do away with widespread use of specific anti-virus software.

The other basic misconception in Mr Schwartau's article is that even if an organisation would in fact need only a single copy of the system manager's favourite anti-virus package, industry would save money: not so. The virus research work would have to be done anyway. This work is currently undertaken by under 100 serious researchers, who share a lot of their results despite the fact that most of them are paid by private companies. I know of nobody who has become extremely wealthy by writing and selling anti-virus software, although a few people in the industry have been doing rather nicely, so it is my conclusion that the total cost to industry will not decrease significantly, even if users shrink the size of their site licences. The economic correlation assumed by Mr Schwartau simply does not exist.

Apart from the conclusions regarding virus protection this was a good article, and I hope this is a sign of *Virus Bulletin* departing somewhat from the rather narrow niche of computer vira and moving into some wider computer security aspects.

Sincerely yours,

Niels-Jorgen Bjergstrom, M.Sc (Eng), MBA
Computer Security Engineers Ltd.

[*Winn Schwartau replies:*

I'm pleased as punch that someone has the wherewithal to respond to my admittedly controversial, albeit correct, position on using security methods to replace anti-virus software. However, I am somewhat at a loss as to how 'a good article' can simultaneously be 'nonsensical'!

The reference monitor is a tried and proven method of reporting the truth. Although it would be possible to subvert the Reference Monitor on a DOS platform, it is still possible to assign a specific level of trust. As for people getting rich on anti-virus software, get real! McAfee has made millions!

If these are Mr Bjergstrom's only objections to my premise, then I suggest he actually supports my position and would do well to enter a market where there is a wealth of money to be made. Niels, thanks for your thoughts, and perhaps you can see that we really do agree.]

Dear Richard,

I would like to take this opportunity to comment on the review of *Microsoft Anti-Virus* by Dr Keith Jackson, in last month's *Virus Bulletin* (May 1993, pp. 17-19).

The very fact that the software is supplied with DOS makes it likely that it will become one of the most widely used anti-virus packages in the world and the *de facto* standard, regardless of its quality. Precisely for this reason it will be targeted by the virus writers - if there are any weaknesses in the software they will be ruthlessly exploited. Partly for this reason, and partly because many reviewers of anti-virus products seem to be largely unaware of weaknesses due to security holes, much greater emphasis should be placed on such loopholes in the evaluation of *MSAV*.

The review published in *Virus Bulletin* failed to mention the great majority of the ten security problems I have discovered within *MSAV*. As an example of some of the problems in the AV software, consider the following: all one has to do is load certain values into various registers and call any one of three interrupts, and VSafe either has all its features disabled, or is completely unloaded from memory.

I do not wish to give the impression that *Microsoft's* (and *Central Point's*) is the only anti-virus software with security holes. Nevertheless, the fact is that these holes could have been blocked had the software manufacturers given sufficient thought to the matter.

Jackson's review seemed rather optimistic, given the security loophole outlined above and the fact that the *MSAV* scanner scores lower than most scanners when testing either accuracy or speed. Will the software be modified to correct these problems? Minor bugs probably yes. However, blocking some of the security holes would involve a fundamental rewrite of the package, which seems unlikely to happen. It is therefore imperative that users be given a clear idea of exactly what they are purchasing if they decide to use the new *MSAV* software.

Sincerely,

Yisrael Radai
Hebrew University of Jerusalem

Yisrael Radai's paper discussing the problems in *MSAV* in detail has been made available to subscribers of *VB*. Any readers who would like a copy of this paper can contact Victoria Lammer (Fax. +44 235 559935) for a printed copy of the report. Alternatively, readers can Email Yisrael Radai (Email: RADAI@VMS.HUJI.AC.IL) for a copy of the paper as a *Postscript* file or an ordinary ASCII file (please specify which).

PRODUCT REVIEW 1

Dr Keith Jackson

PC Immunise II - Son of *PC Immunise*

PC Immunise is one of the longest standing anti-virus programs. Indeed it was only the second product that I ever reviewed for *VB* (August 1989) - doesn't time fly!

The stated objective of *PC Immunise II* is to 'detect and flag unsolicited amendments to the system very soon after they happen'. What this actually means is that the software attempts to spot changes to the system by detecting the creation, amendment, or deletion of files and subdirectories, by verifying that checksums calculated across a file's contents are unchanged.

The review copy of *PC Immunise II* was provided on both 3.5 inch (720 Kbyte) and 5.25 inch (360 Kbyte) floppy disks, both of which arrived in write-protected form. The latest file creation date of any of the *PC Immunise II* files was 9th September 1992, but as the product is an integrity checker this is not necessarily a cause for concern.

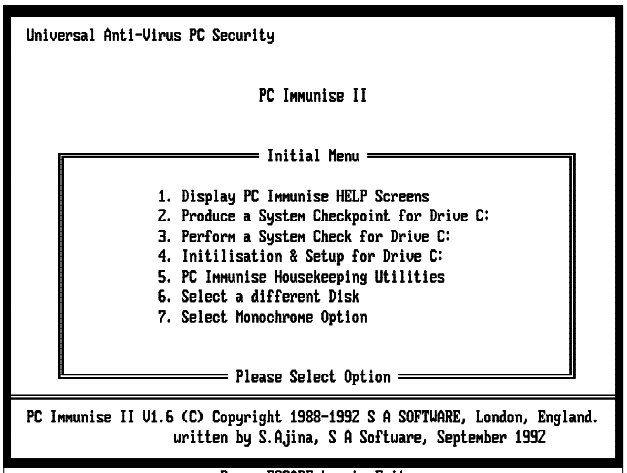
Documentation

The manual provided with *PC Immunise II* was unfortunately rather old (dated September 1990), and various inserts have been added to correct the text where the program has advanced. At just 55 pages of ringbound A5, it does rather spoil the appearance of a product if the developer cannot keep such a small amount of documentation up to date.

The manual does not contain an index. As I have stated before about other products, the lack of an index makes a manual close to useless when searching for specific pieces of information. Even given the above criticisms, there is no doubt that the manual has improved.

The manual contains a legal disclaimer which states that *SA Software* does not warrant that the operation of the program will be uninterrupted error free'. Make of that what you will, but one thing is for certain: it is not a clause that is routinely inserted by other program developers. I am very suspicious of this type of clause, and react badly to its insertion - it hardly inspires confidence in a product. Still, this is an improvement on the 1989 version, which disclaimed 'any fitness for any particular purpose'.

Installation of *PC Immunise II* is simple: just copy all of the files into any desired subdirectory, and type IMMUNISE. The menu-driven shell program then appears and offers various choices, one of which is to install *PC Immunise II* onto a specific drive, in a specific manner. An on-line help system is provided which is very thorough, splits readily into various sections and is easy to use.



PC Immunise II now offers users a menu-driven front end. The on-line help facilities provided are very good, and help make up for the problems with the manual

Variable Levels of Protection

The manual contains a good discussion of recommended detection levels and, given the complexity provided by the myriad options, this is definitely necessary. By way of a short explanation, a user of *PC Immunise II* must decide whether he wishes to use *PC Immunise II* at a 'Low', 'Medium' or 'High' level of detection.

'Low' just detects changes to the system software and the operating system. 'Medium' does all the checks prescribed for 'Low', and also looks for new hidden files and changes to existing hidden files. 'High' does all the checks prescribed for 'Medium', and also identifies changes to the files and/or subdirectories.

Just to confuse matters even more, the 'Medium' and 'High' levels are each further subdivided into 'Normal' and 'Extended' modes, where 'Extended' checks a file's entire contents, and 'Normal' only looks at the file's size, date/time stamp, and attributes. After all this has been decided, when Extended level is chosen, the user must decide if this should apply for all executable files, all executable/system/overlay files, all files containing one of a set of extensions specified by the user, or all files. Up to 4 subdirectories can be omitted from these tests, and this too must be specified by the user.

I have gone into this in some detail to make the point that this is not a product which can be used without much thought (as most scanners are used). Quite a lot of planning

must go into its use, especially when time taken to execute is a relevant factor (see below). When new or amended files are detected by *PC Immunise II*, the user can view, search and delete these files. In common with most 'change of setup' functions, such options are password-protected.

New Look

PC Immunise used to be solely a command line-driven program, with various command line parameters used to initiate the setup process, recalculate the checksums, and/or verify that the checksums are correct. This method of operation is still available, but a shell program is now provided which allows parameters to be set by making a selection from a menu.

However this 'shell' program insists on returning to the operating system prompt after every execution of a component of *PC Immunise II*, rather than staying within the menu-driven shell to allow more program usage. This is frustrating to say the least.

Various date/time test utilities are also provided which can either be used from the menu-driven 'shell' program or as stand-alone utilities. They return error levels and can be used to construct complicated batch files as an aid to automating the process of checking whether a disk has been corrupted.

Scramble And Scatter

At its higher levels, *PC Immunise II* uses a checksumming process to detect changes to a file, and can detect changes no matter how they are caused (by a virus or otherwise). When it first examines a disk, *PC Immunise II* creates a database of two hidden data files in the root directory of the disk. I have no idea why two separate files are created. The data in these files is stored in encrypted form, though the documentation hardly inspires confidence when it states that 'The information held by *PC Immunise II* is stored using proprietary Scramble and Scatter techniques'. Technically, this is a content-free statement.

The *PC Immunise II* data files are called IM UNISE.DAT, and IM UNISE.2DT (note the space between the letters M and U in the middle of each file name). This space makes it impossible to enter the file name in a DOS command, even if wild-card characters are used, and coupled with the files' Read-only, Hidden and System attributes, accidental alteration of either of these files would seem to be very unlikely - a useful feature.

Details of the algorithm used by *PC Immunise II* to calculate its checksums are not disclosed by the developer, which prevents any comment on the cryptographic strength of the algorithm. To prevent reverse engineering, a checksum algorithm should have reasonable cryptographic merit, but the documentation provided with *PC Immunise II* merely states that 'checksums are obtained using an internal proprietary *PC Immunise II* algorithm. The checksums are not simple sums of all bytes'. The fact that the developers even thought that the last sentence was necessary makes me rather concerned about the cryptographic strength of the checksum algorithm.

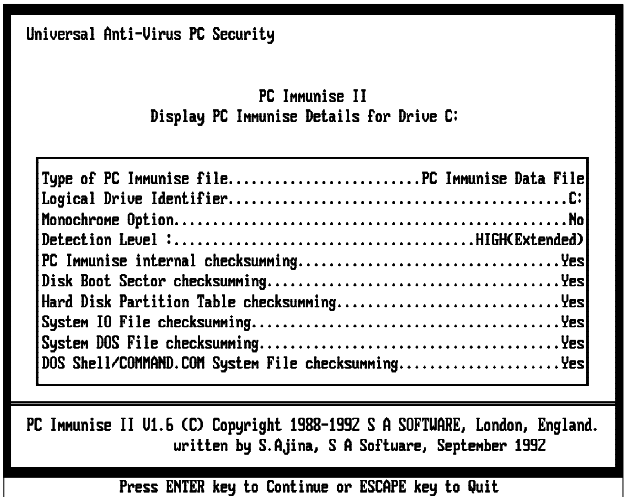
As I do not know what the algorithm is, and cannot readily deduce it from *PC Immunise* operation, I cannot comment on its strength. Neither can anyone else - the user is at the mercy of the developer's expertise on this point.

When *PC Immunise II* is first used on a bootable hard disk, it requires that an original master floppy disk for the particular operating system version in use is available, as it confirms that the operating system files on the hard disk have not been corrupted in any way. Although this seems to be a drudge, it enhances the security provided by *PC Immunise II*, and the developers should be applauded for bothering to include it (most other checksummers do not bother).

After installation I tested *PC Immunise II* against various file alterations and it proved capable of detecting every single bit change to a file, the creation of a new file and deletion of an existing file: excellent.

Speed Tests

The time taken by *PC Immunise II* to execute while using various detection modes proved rather illuminating. Unless mentioned otherwise, all timing figures were measured on my *Toshiba 3100SX* laptop (see *Technical Details* section) with a hard disk containing 27.1 Mbytes in 724 files (298 of



PC Immunise II is a flexible integrity checker, but without publishing the algorithm, it is impossible to assess its security.

the files are executable files, occupying 12.8 Mbytes) on a drive compressed using the *Doublespace* utility provided with v6.0 of *MSDOS*. Note that although I referred earlier to the fact that the *PC Immunise II* program has not been updated since September 1992, it coped with *MSDOS v6.0*, including the *Doublespace* compression.

At the 'Low' level of detection, all checks happened so quickly that the actual time taken was just a couple of seconds. This was not worth measuring compared with what is coming below! When *PC Immunise II* was used at the 'Medium' level, 3 minutes 59 seconds was required to verify that the disk remained unaltered, no matter whether a full system check was selected or simply identified amended files. When used at the 'High' level, the time taken for either a 'Normal High' test, or an 'Extended High' test, was 4 minutes 1 second in either case. Note that effectively all 4 cases take the same time to execute.

I tried the above test when *PC Immunise II* was executed under *Windows v3.1*, and the time to do a system check of executable files only rose to 4 minutes 4 seconds, a very small increase over the bare DOS performance. Remember that these times are reported on a machine that is not unreasonably slow (a 16 MHz 386), with only a fairly small hard disk (just under 13 Mbytes of executable files). The timings would scale linearly with disk size, therefore any disk which contains a few hundred Megabytes of files is going to take a *long* time to check using *PC Immunise II*.

For comparison purposes, I ran the same 'High' level test on an old XT computer. This took 10 minutes 15 seconds when only executable files were included, and when I extended the scope of the test to include all files on the hard disk, *PC Immunise II* took 34 minutes 20 seconds to complete its check. I would contend that either of these figures prevents *PC Immunise II* from being used seriously on a slow PC at anything other than a 'Low' level of detection. Remember that the 'Low' level of detection only checks the operating system's files which is probably good enough for most users.

Implications

The timing problems with *PC Immunise II* actually point out a more subtle problem than the program's slow execution speed. I reported above that the time taken to check a disk was almost identical at the 'Medium' level and the 'High' level of detection.

As I understand it, the basic difference between these two levels of detection is that the 'High' level includes verification of a checksum calculated across the entire content of a file. Therefore the claims that a secure checksum algorithm is being used are almost certainly not true - otherwise the time taken in the two cases would be markedly different. In my humble opinion, the checksum algorithm cannot be doing very much if it takes hardly any time to perform its action when applied to every single byte in a file.

Of course, I cannot prove this conjecture unless the developers publish details of their checksum algorithm, and prospective purchasers should draw their own conclusions from the results reported above.

Believe it or not, I actually have a problem with this product's name. In the anti-virus field, the word 'immunise' has come to mean adding code to a file so that when executed a program can itself detect any alteration to its contents. *PC Immunise* was written before this usage, so it is not really the developer's fault. Nevertheless, it may not be what a prospective purchaser anticipated. *Caveat emptor*.

Conclusions

My conclusions on *PC Immunise II* have not really changed too much in 4 years. It does detect changes to files and/or the operating system, but the user must pay quite a time penalty when *PC Immunise II* is used at any of its non-trivial levels. The checksum process itself is still clouded in mystery as no details are released by the developer, which makes it impossible to judge its security. However, given the almost identical times for various different modes of operation, I somehow doubt that the checksum algorithm is doing very much.

PC Immunise II is a more mature product than the version that was reviewed 4 years ago, it has improved a lot in terms of how the three basic modes of detection are controlled. In my view *PC Immunise II* really is too slow for routine use at its more secure levels of operation - but that's a subjective judgment which the user must make for himself by trying the product on his own hardware.

Technical Details

Product: *PC Immunise II*

Developer and Vendor: *SA Software*, 28 Denbigh Road, London W13 8NH, UK, Tel: +(81) 998-9918 or +(81) 998 2351.

Availability: PC, XT, AT, PS/2 or compatible using DOS 2.0 or higher. 420 Kbytes of RAM is required. PC-DOS, MS-DOS, DR DOS and UNISYS DOS are all supported. *PC Immunise II* will execute under *Microsoft Windows* v3.0 or later.

Version evaluated: 1.6

Serial number: 91368B

Price: £34 per PC for single copy. Site licences available.

Hardware used:

a) *Toshiba 3100SX*, a 16MHz 386 laptop, with 5 Mbytes of RAM, one 3.5 inch (1.44M) floppy disk drive, and a 120 Mbyte hard disk, running under *MS-DOS v6.0*. (b) 4.77MHz 8088, with one 3.5 inch (720K) floppy disk drive, two 5.25 inch (360K) floppy disk drives, and a 32 Mbyte hard card, running under *MS-DOS v3.30*.

PRODUCT REVIEW 2

Launch *The Interceptor!*

This month's review examines a product which is somewhat different from the usual array of scanners and integrity checkers. *The Interceptor* has clearly had to battle against the preconceptions of reviewers, as the covering letter explains carefully that the product is not a scanner, thus making it harder to test - no running it against the standard battery of viruses this time!

The Interceptor claims that it offers a new way to combat viruses and that 'the need for constant, continuous and regular updates is drastically reduced'. Moreover, that 'in the majority of cases, *The Interceptor* will handle new attack strategies without faltering'. Users have heard claims like this many times over - can *The Interceptor* live up to them?

Multi-partite Manual

The Interceptor product consists of an A5 comb-bound manual and a single 720 Kbyte 3.5 inch floppy disk. Although the disk arrived write-protected, the write-protect tab was still in place. Far better would have been a permanently write-protected master disk - it is all too easy for someone to slip the tab across inadvertently.

The manual begins with a brief overview of the design and aims of *The Interceptor*. The manual is honest and does not attempt to gloss over the problems which anti-virus vendors face. Indeed, the first page of the manual explains that 'No knowledgeable anti-virus researcher would claim that this, or any defence cannot be defeated'.

The manual then goes on to explain in detail how to install, run and remove the product from the machine. The most useful section is one of the appendices which explains that the best defence against computer viruses is better hygiene rules on the part of the user.

The index is complete, but badly organised: do users really want thirty nine references to Product Installation? A more detailed index with fewer entries would be far more use: the current offering looks like something produced after doing a text-search through the manual.

The other complaint about it is its lack of robustness. After only two days use, the manual had split itself up number of component parts - this was due to the holes for the binder being too close to the edge of the page. One dreads to think how it would fare over six months in a busy working environment. This could easily be improved.

Installation

The installation instructions are relatively clear and easy to follow. The user is first advised to install the product from a copy of the original, and to ensure that the disks are always write-protected. One is then required to copy the contents of the floppy disk onto the hard drive.

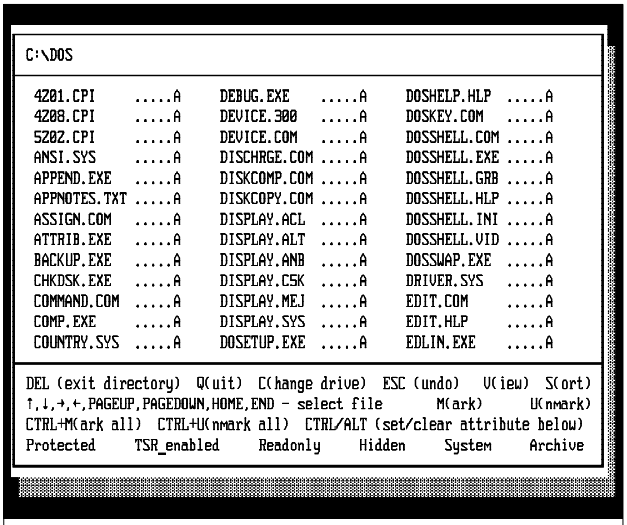
The next step of the process is to create a bootable system disk, using *The Interceptor's* MAKEINST program. The program is then installed from this newly created system disk. The whole process is a bit confusing - surely this process could be automated to a higher degree?

Once the machine is rebooted from this installation disk the user is presented with a simple menu system, which allows him to select an installation identity and choose where the software should be installed to on the hard drive.

The PC is then rebooted normally from the hard drive. In the test, the machine booted and then attempted to load Smartdrive from AUTOEXEC.BAT... at which point it hung. A quick look through the manual showed that this was due to 'an unauthorised program attempting to become a TSR'. The machine had to be rebooted from the installation floppy, and the attributes for this file were reset (see below).

Boot Sector Protection

The Interceptor is basically a combined behaviour blocker and integrity checker. The idea is that once it is installed on a hard drive, programs which display virus-like behaviour are not allowed to execute. This means that programs which become memory-resident, or attempt to modify certain sections of the hard drive will not function correctly.



The FILER utility provides a quick and easy way to alter the attributes of files stored on the disk.

The first point to note is that the installation disk also doubles as a rescue disk. Once *The Interceptor* is installed, the hard disk is no longer accessible when the machine is booted from an ordinary DOS System disk. Therefore most DOS Boot sector viruses will not be able to infect the boot sector, as the partition boot table is not accessible. Most Master Boot Sector viruses do not take the partition table into account, and will infect the disk anyway.

The Interceptor claims to be aware of this, and is capable of disinfecting the hard drive if any changes are found. The technique it uses to avoid being 'stealthed' by the viruses is not made clear in the documentation. Whichever way it is done, it certainly appears to be effective: *The Interceptor* successfully detected and removed all the common boot sector viruses, including Form, Spanish Telecom, New Zealand 2, NoInt and Italian.

The way the product handled the EXEBUG viruses was particularly impressive: not only were both variants of the virus removed, but the contents of the CMOS were reset to their original value - a result far better than many virus scanners could achieve!

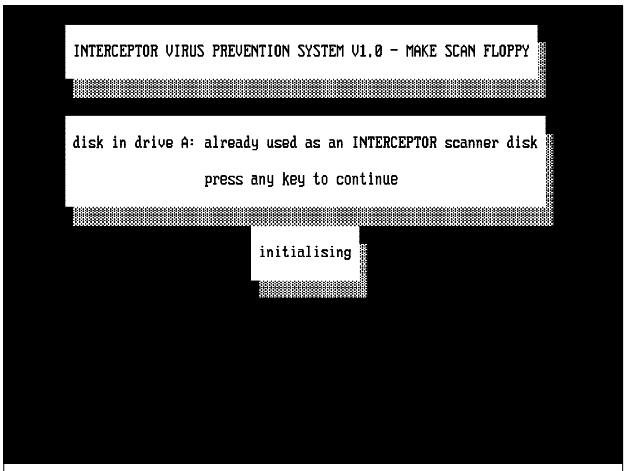
My only complaint with the handling of the boot sector infections is that the user is never informed that a virus was encountered. When the machine boots up, *The Interceptor* indicates that it is attempting to repair the disk by displaying a single-character rotating bar on the screen. It then forces a reboot. There is always something more interesting to do than watch a somnolent PC boot up first thing in the morning, and this tell-tale sign could easily be missed.

There is certainly a case for the user to be informed that the boot sector of the hard drive had been changed - after all, nobody wants an infected disk loose around the office - even if the machines are all nominally protected! *VB* is assured that this will be added in the next release.

File Infectors

The Interceptor claims to provide protection against file infectors as well as boot sector viruses. Protected files cannot be renamed, deleted or have their size changed. Limited cover is allowed for unprotected files.

It was here that some of the limitations of *The Interceptor* became apparent. One of the standard tests of packages of this type is how they deal with self-modifying code (such as the SETVER program, which is part of MSDOS). The manual states that such software is incompatible with *The Interceptor*, and tests certainly showed this to be the case: using SETVER caused DOS to display a box containing the message 'A serious disk error had occurred', and offers an abort or retry option.



The menu interface used by *The Interceptor* is stark but functional. However, in day-to-day running the user should never even need to know about it!

The Interceptor performed well against memory-resident viruses, as it successfully stopped DIR II, 4K, Cascade, Tremor, Eddie and Eddie II before they had infected anything. In fact only one virus out of the thirty-something memory-resident viruses tested (SVC 6.0) managed to get around the protection.

Unfortunately, non-resident viruses had a much easier time. Every 'single-shot' infector was successfully replicated (eg the Aids virus, Tpworm etc) even though *The Interceptor* was nominally protecting the disk. However, no files specifically marked for protection were successfully infected.

Filer

The way *The Interceptor* protects the files on the hard drive can be configured using a utility named FILER. This program allows the attributes of files to be altered and set.

Using FILER is very easy as its interface is very similar to disk management programs like *Xtree Gold*. The user can navigate around the package using the cursor keys to select files for alteration. In addition, there is a key to tag all files in a particular directory for the same treatment.

No problems were discovered when using FILER, and in all cases marking TSR files as 'TSR enabled' allowed the file to be used normally. Unfortunately there is no option to exempt certain files (such as SETVER) from protection, and they will not co-exist happily with this product.

Scan Disks

The authors of *The Interceptor* are clearly well aware of the need to clean boot a machine if a scanner is to be run. Once *The Interceptor* is booted from a vanilla DOS disk, any

scanner which examines the disk will be unable to operate correctly. For this reason an option to create a bootable 'scan disk' is included.

The user is instructed to format a bootable system disk, and then execute a program called MAKESCAN, which creates a boot disk which is capable of reading drives protected by *The Interceptor*. All this worked fine, and after waiting for about a minute, *The Interceptor* produced an *'Interceptor* aware' bootable disk, as promised.

In an attempt to counterstealth viruses, some scanners will attempt to tunnel the 'original' Int 21h and Int 13h vectors, and make system calls directly to the ROM. Jim Bates has a program which attempts to gain access to Int 13h in one of several different ways. Using this program it was possible to strip the original Int 13h call back in to the ROM. Therefore any scanner which uses this technique may be unable to access the data stored on the hard drive.

Disk Problems

The biggest dangers of using any software which meddles with the hard disk at a low level is that in the event of something going wrong, users can find themselves in big trouble. Unfortunately, this is exactly what happened.

One of the viruses used for test purposes was SVC6.0. This is a multi-partite virus which is capable of infecting the Master Boot Sector of the hard drive. When an infected file was run, the machine appeared to function normally, and the virus became memory-resident.

Things became worse when the machine was rebooted. The contents of the CMOS had been corrupted, and the machine would get half way through its boot process and then hang. The manual advised me to boot the machine from *The Interceptor* rescue disk and use the 'Check/Repair Installation' menu. When *The Interceptor* searched for an Installation ID none could be found, and the package asked for an identity from which it would attempt to recreate the disk. This failed.

The Interceptor was not capable of repairing the drive or the damaged CMOS, and the normal disk recovery tools which one could use (such as *Norton Disk Doctor*) were confused by the corrupted partition information stored within the MBS. After an hour of fiddling about, it became apparent that quickest option was to reformat the drive and re-install DOS - thank goodness this was a test machine!

System Load

Obviously the checks which *The Interceptor* makes on the system must load the system. Before installing *The Interceptor* on the test machine, the system speed was evaluated using *Norton's System Information* utility (v4.50). This returned a *Disk Index* value of 2.3 when *The Interceptor* was active, and 5.9 on the plain DOS system - a sizeable difference (this is over a 60% drop!).

How this matters is an open question - on disk intensive operations such as when running *Windows*, this may become significant. In addition, the result obtained by *Norton* can be slightly misleading and no delay was noticeable on the test machine.

Conclusions

The Interceptor is a rather puzzling product. It certainly contains some highly innovative and clever code, and is good at detecting programs which become memory-resident, but it does not provide adequate protection against non-resident viruses, unless unless every executable file is earmarked for special attention.

The biggest problems arose when attempting to recover a disk - *The Interceptor* would not recognise the hard drive, and did not provide adequate functionality in these circumstances - this needs to be improved.

The automatic removal of boot sector infections is a useful feature, which may make the product extremely useful on stand-alone machines in a computer room, but other than that, I am at a loss to see the target market.

Overall, *The Interceptor* was very good at dealing with the more common viruses and its handling of boot sector viruses was excellent - some manufacturers could learn a lot from this. In addition, the manufacturer has assured *VB* that it will address many of the criticisms raised. If this is the case then *The Interceptor* will certainly be worth another look in future incarnations. However, the problems with the hard drive, coupled with the fact that certain viruses can circumvent its protection mean that users would be well advised to consider carefully the pros and cons of their choice.

Technical Details

Product: *The Interceptor*

Developer: *The Alpha-Omega Group*, PO Box 6079, Dunedin, New Zealand. Tel. Not Supplied. Fax. (+643) 473 7295.

Availability: Not explicitly stated

Version Evaluated: Version 1.00

Serial Number: 10014

Price: $100 per PC.

Hardware Used: 25Mhz 80386SX *Opus Technologies* desktop machine, with 4MB RAM, one 3.5-inch (1.44M) floppy disk drive, one 5.25-inch (1.2MB) floppy disk drive, and a 100 MB hard drive, running DOS 5.0.

FEATURE

Mark Hamilton

Have Modem, Will Travel

Several years ago, it would have been unthinkable to dial a Bulletin Board in order to obtain information about computer security and computer viruses. The very thought of it would send a shiver down the back of any self-respecting corporate. Even now, Bulletin Board Systems (BBSs) are more or less off-limits for employees, as managers are concerned that by allowing unrestricted access to BBSs, staff will become less productive as they find interesting topics in other areas and, far worse, might introduce some 'nasty' or other into the company's computer system.

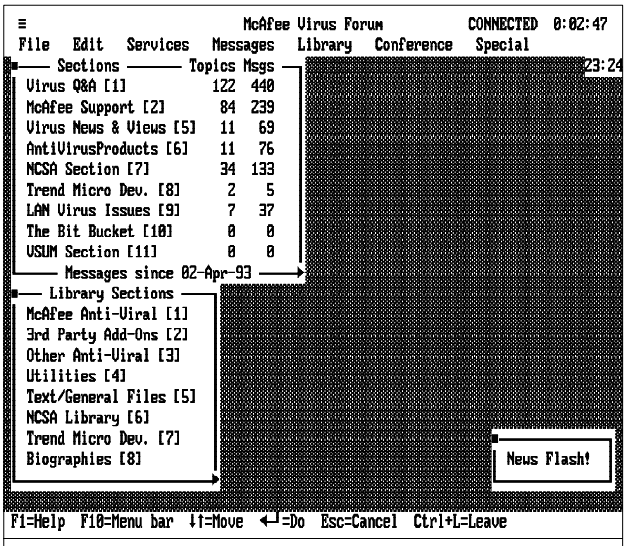
Even though both of these arguments are not without merit, the larger BBSs do provide essential services to some. Help is certainly out there - if only you know where to look!

Technical Support

I remember discussing this very topic in January, with a senior computer consultant working in the oil industry in London. His company has made the decision, for better or for worse, to standardise on *Microsoft* products. If you, as both he and I have done on many occasions, have ever tried to obtain an answer from that company's technical support department, you will understand his sense of frustration.

First you need a touch-tone phone. Next, you press an endless stream of digits as you are prompted by the pre-recorded voice and then you wait in a queue. It could be several minutes before you actually get to speak to a human being and then, the chances are, your problem will not be immediately resolved. You too will soon seek an alternative means of getting information, assistance and support. In this situation BBSs can provide the answer.

In the United Kingdom, a number of the anti-virus companies run their own Bulletin Board Systems - including *IBM*, *Total Control*, *Central Point* and *Sophos* - but these primarily exist for solving problems relating to their own products. If you want information of a more general nature, to assist with formulating your company's anti-virus strategy for example, you have to look to either *CompuServe*, *Compulink* (*CIX*) or the Internet to satisfy your needs. Our American cousins are somewhat more fortunate - as well as *CompuServe* and Internet, there is also *America OnLine*, *BIX* (*BYTE Magazine's* BBS), *Prodigy* and their various associated information providers.



One of the most popular virus forums available on *CompuServe* is the Virus forum run by Aryeh Goretsky and Spencer Clark. However, be warned - it is very easy to run up large bills!

One of the benefits of using BBSs is that there is a good chance that someone else (who may not even work for the software company) will have come across your problem and can post a reply for you very quickly indeed. It is not uncommon to post a question before lunch and to have a number of replies by that evening.

CompuServe

CompuServe is probably the world's largest BBS and is accessible from most countries either directly through a local node or over a PSS network. England currently has three *CompuServe*-owned nodes, in London, Reading and Bristol, and, in addition, there are a large number of local PSS Dialplus numbers available.

CompuServe itself has its headquarters in Columbus, Ohio where there are a large number of custom-built DEC 10 and DEC 20 mainframes which act as the host machines (although there are also host machines in other US cities) and they are all interconnected in a high bandwidth network.

In the main, *CompuServe's* forums are run independently of *CompuServe's* direct control by vendors and other interested parties who receive a share of the revenue generated.

Several of the principal US anti-virus vendors maintain forums, including *Central Point* and *Symantec*, but by far the most popular seems to be that run by *McAfee Associates*. Part of its forum is run by the *NCSA* and it addresses both virus and non-virus related security issues. Aryeh Goretsky and Spencer Clark, the two *McAfee* Sysops (System Operators) manage to field both general questions on viruses as

well as those relating specifically to *McAfee's* various anti-virus offerings. Since this company's products are Shareware, the latest versions are always available for downloading.

In the past, I have been a frequent visitor and participant in this forum and can vouch for the fact that the quality of the information is generally good. However - and this applies to all forms of communication - you only get out of a system what you put in. In other words, the more you contribute, the more you learn. This maxim is especially true of *CompuServe* and all other BBS systems.

McAfee's forum, because it is called VIRUSFORUM, does attract users of rival products and its Sysops found that they were expected to answer technical questions relating to its competitors' products. For this reason, they display a message to direct *Central Point* and *Norton*/*Symantec* users to the relevant forums.

You can access *CompuServe* interactively using a normal comms program such as *Procomm* or *Telix*, though this is not recommended. There is an interactive program called *CIM* (*CompuServe* Information Manager) for DOS, *WinCIM* (a *Windows* 3.x equivalent) and *MacCIM*. These use a special Host-Micro Interface (HMI) which means that you can read messages while downloading a file or participating in an on-line conference, or talk session, with other users. The various *CIM* products are the only ones that allow you to do all these things concurrently, but as you are connected on-line all the time, it can get quite expensive.

A more usual way to do the messaging and file downloads is using one of the various navigator programs. These download the messages into a database, allow you to read and reply to them off-line and then upload the replies. There are several, mainly Shareware, available including *TapCis*, *OzCIS* (my personal favourite) and *TeePee*.

CIX

Compulink (CIX) is hosted on large Unix micros and uses a version of CoSY - the same conferencing software that *Byte* Magazine's *BIX* uses. The virus conference is usually quite lively though, and questions are usually answered quickly.

CIX is an extremely useful meeting place for users of any of *S&S's* products, as they have their own support forum there, from which users may download bug fixes and additional patterns for *Dr Solomon's AVTK*.

As an information source, *CIX* is a poor cousin to *CompuServe* - it simply does not have the same user-base. However, in its favour, *CIX* is much easier to use and does not need a navigator program, though it is easier to use with one. I frequently log-on to *CIX* using the Shareware comms program *Telix*. There are navigators available - the two most popular are *Matrix* and the *CIX* version of *TeePee*, but neither are up to the standard of their *CompuServe* counterparts because of the more restrictive hosting software.

The Internet

For users seeking the truly independent word, neither *CIX* nor *CompuServe* can provide the solution, which is a great pity. As a source of independent and unbiased information, the Internet seems the obvious choice, but unless you're fortunate to be associated with a University and can access it through JANET (the Joint Academic Network), then in this is going to cost you money (rates start at around £10 a month). In the US there are a number of companies who can provide dial-in facilities to the Internet at highly competitive rates - and it pays to shop about.

The Internet is enormous - and almost anything which can be stored on computer is available here - if you can find it. Most of the shareware virus scanners can be downloaded by FTP from various internet archive sites, and many vendors have Email addresses, allowing questions to be put directly.

However, the best source of information on viruses is the Internet Newsgroup comp.virus. This provides an independent source of information - if you want to know about the Form virus, than all you have to do is ask. The only drawback is that the information you may receive is not always completely accurate.

In the majority of cases though, the Internet provides an excellent way to share problems and solutions with a wide cross section of people - including various experts and names from the field. It is not uncommon to have your query personally answered by Vesselin Bontchev, Fridrik Skulason or some other 'name' from the industry.

Conclusions

There is a great deal of help available to the curious - all one needs is a modem and a handful of useful telephone numbers. For the less experienced user, the best placed to start is *CompuServe* - its wide range of vendors and active conferences provide an ideal place to learn how to get the best out of Bulletin Board systems. However, if you have Internet access, the Newsgroup comp.virus is active enough to satisfy most minds, and is only the tip of an iceberg when considering the wealth of information stored on various archive sites.

The basic rule is that there is plenty of information available out there - often supplied by some of the best known names of the anti-virus community. If you have free Internet access then it does not cost you a penny, so why not get involved?

END-NOTES AND NEWS

3rd International Virus Bulletin Conference 9th-10th September 1993, Amsterdam, The Netherlands. Contact Petra Duffield. Tel. +44 235 531889.

It has been a busy month for the *Novell* Certification test labs. This month, both *Sophos Ltd* and *Central Point* have announced that their products have achieved the heady status of ***Novell* 'Tested and Approved'** products. Not to be confused with the lesser badges which announce 'Yes, it runs with *NetWare*', the certification means that there is a better than average chance they will not crash your file server. For further information contact *Sophos Ltd*. Tel. +44 235 559933 and *Central Point*. Tel +44 81 848 1414.

The certification of the *Central Point* product coincides with the company **dropping the price** of the NLM from £699 for a single server with up to five connected workstations to £699 for a single server with unlimited workstations. This means that the saving offered to a typical small business site with fifteen workstations operating from one server would be approximately £750. Tel. +44 81 848 1414.

June 9th is to become the first ever **American 'National Virus Awareness Day'** . The event is jointly sponsored by the *NCSA* and *3M*. According to Virginia Hockett, Information Technology manager, *3M Memory Technologies Group*, 'Reputable computing requires that users be aware of the simple means of protection at their disposal. This also means that media manufacturers - and, for that matter, all major players in the computer industry - have a responsibility to adopt, enforce and advocate safe computing practices.' For further information Tel. +1 (717) 258 1816.

***Visionsoft* has announced the release of a new packaging deal** called 'Security Blitz' which contains five of *Visionsoft's* most successful products in one package, including access control, backup software and anti-virus software, for £147. Tel. +44 274 610503.

S&S International has announced that it intends to **extend its 'competitive upgrade' policy** to include users of *MS-DOS v6*. This allows purchasers of the new version of DOS to buy a copy of *Dr Solomon's AVTK* for only £49.95 - less than the upgrade price for *MSAV*. Tel +44 442 877877

Whatever next. **A computer in the United States has been found in contempt of court** after it repeatedly sent 'no balance due' notices in error. Judge Cristol issued a contempt citation against the offending IBM microcomputer, fining it 60Mbytes of memory! No model was specified in Judge Cristol's order, and so the fine was settled by having a hard disk and nine microchips delivered to Judge Cristol's courtroom. The possibilities of applying this ruling to computer viruses are endless...

STOP PRESS: For some months now, *Virus Bulletin* has been aware of a Virus Exchange Bulletin Board being run on a machine owned by the US Department of the Treasury. However, the BBS has not been mentioned, as it was felt that attracting uneccessary publicity for it would be counterproductive. Due to pressure from within the industry the BBS system has now been closed down, although the SysOp has stated that he will attempt to further the activities of the board through other channels.

VIRUS BULLETIN

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, 21 The Quadrant, Abingdon Science Park, Abingdon, OX14 3YS, England

Tel (0235) 555139, International Tel (+44) 235 555139
Fax (0235) 559935, International Fax (+44) 235 559935

US subscriptions only:

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

Tel 203 431 8720, Fax 203 431 8165