August 1989 ISSN 0956-9979

VIRUS BULLETIN

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

CONTENTS

EDITORIAL

The heatwave continues here in the UK and in the *Virus Bulletin* office the bets have been placed as to which will melt first - the computers or the editor. Most of the calls have been routine in nature. Occasionally, however, a call comes in from a site infected by a computer virus or someone offers to send us a disk which they suspect to be a virus carrier. Most encouraging, is the fact that *Virus Bulletin's* IBM and MAC tables are actively being used to discover live viruses in computer systems.

The Known IBM Virus Table has expanded considerably since the last edition. In the Seen and Disassembled category there is a significant number of new entries. All viruses which appear in the tables, even those which seem innocuous, represent a major threat. Remember it is the replication mechanism of these programs which is so difficult to write. Changing the virus side-effect is relatively easy - for example, it takes only five assembler instructions to destroy a hard-disk. The message here is that once virus code is in circulation any number of different effects can be added to it.

It is interesting to note that during this period of IBM PC virus proliferation things have remained stable on the Macintosh front. The Known Macintosh Virus Table remains unaltered at the time of publication. Mac users may like to know that a *Virus Bulletin* technical review of the new Symantec Antivirus for Macintosh (SAM) is in the pipeline.

Speaking of products, congratulations to Dr. Fred Cohen and his product Advanced Systems Protection which recently won an award from the Institute of Chartered Accountants in England & Wales. The award was for the best initiative or product to combat the computer virus threat. One entry was from a fourteen-year-old schoolboy which is as impressive as it is perplexing. It is a pity that no details were released of the testing protocol necessary to select the winning product or initiative. Andrew Oakley, chairman of the judging panel, outlined to me some of the difficulties of assessing the relative merits between ideas and products. Still, it would have been nice to have had some criteria layed out before us.

We had planned to run an evaluation of ASP in this edition of *Virus Bulletin*. This has been delayed and will feature next month.

The promised dissection of the Datacrime virus appears on page 12. It is very difficult to assess just how widespread this destructive virus is. The variants we have seen and disassembled originated in the United States and Holland, and we have had no reports of it being discovered here in the UK. The virus is currently in its dormant phase and crude statistics will only become available after 13th October. Note that Datacrime will trigger **after** 12th October, i.e. from 13th October onwards.

Finally, the preliminary report on Traceback has been postponed, a full report will appear in September.

TECHNICAL EDITORIAL

Joe Hirst

Virus Bulletin has not received permission to reproduce this article on CD from the author. Readers can obtain a paper copy of the original issue directly from *VB*.

CASE STUDY

Jim Bates

Italian Virus in Action

I was recently asked for some advice concerning a suspected virus infection at a firm of accountants. One of the senior partners telephoned me and said that for several weeks they had had sporadic outbreaks of a "full stop" bouncing around the screen on one of their PC machines running Wordstar. "I don't think it's serious", he said, "but I would like your advice because we are now getting the same effect on another of our machines". I don't run any sort of commercial "virus killing" service, but I **am** interested in viruses and since the accountants' office was reasonably near, I agreed to call around to see them and examine the problem.

The office uses five IBM PC compatible machines, all located in the same open-plan area. I spoke to the operator on the first affected machine, and asked her to tell me the history of the problem. She first remembered seeing the bouncing dot some weeks previously but took little notice of it because she considered it to be another "joke" program which some of the junior members of staff were fond of loading onto her machine. When I enquired about this, she explained that some of the staff had their own PCs at home and they had accumulated a number of games and joke programs - one in particular resulted in little "faces" running around the screen regardless of what program she tried to run. When the bouncing dot first appeared, she had assumed it was a similar type of program and had simply rebooted her machine to clear it. Over a period of time, it had become apparent that no one was deliberately loading such a program and the bouncing dot continued to appear on this machine at intervals of roughly twice a week. Rebooting the machine usually cleared the problem and no problems had been noted with the overall machine operation. The second machine had only recently started to display similar symptoms but the problem seemed more acute since the dot made much more regular appearances.

I checked the first machine using a utility program similar to Debug and confirmed that the machine was infected with the Italian virus. This is a boot sector virus and can be recognised quite easily by the presence of the virus' own recognition code of 1357H at offset 1FCH into the hard disk boot record. Removal of this virus is quite simply a matter of backing up all the files on the disk and then reformatting it after booting from a known clean copy of a system disk. The office kept an excellent and up to date sequence of backup floppies so I was able to reformat and reconfigure both disks within an hour. Once the machines were clean, I inserted the virus recognition code* (1357H at offset 1FCH of the boot record) in an attempt to thwart any future infections of the Italian virus. I also installed a virus detection program to take care of any potential parasitic infections.

With the machines up and running normally again, I asked to speak to the staff generally and after some questioning it transpired that they had developed a habit of playing computer games during their lunchbreak. Most of these games could be copied onto the machine's hard disk but there were one or two which required the booting of a floppy disk to get the game started. This was obviously where the infection had entered their system so I gave them all a leaflet about computer viruses and how to avoid them. I suggested that there was nothing wrong with playing games, but only if they were bona-fide programs from a reliable source.

Fortunately, the office generally did not make use of system floppies and to avoid the possibility of someone accidentally attempting to boot a machine from an infected data disk (thus possibly re-infecting it), I set up a "clean" write protected system floppy disk for each machine and instructed them always to boot the machine from it. This method of protection against boot sector viruses is very effective, particularly if no system is placed on the hard disk (thus forcing the user to use the boot floppy). It is however necessary to include the line:

```
SET COMSPEC =C:\COMMAND.COM
```

within the AUTOEXEC.BAT file to avoid the "Insert System disk in Drive A:" messages that otherwise occur.

I finally explained to all concerned that although the Italian virus does not damage files, the same infection route used by another virus could easily have deleted vital data and caused the firm much aggravation.

* Note: This could only be done because the user would no longer be booting from the hard disk (see page 9) (Tech Ed)

KNOWN IBM PC VIRUSES

Joe Hirst

The following is a list of the **known** viruses affecting IBM PCs and compatibles, including XTs, ATs and PS/2. The list consists of two parts. Aliases and descriptions are now in the first part of the table and this is followed by information for programmers. The second part includes the infective length (amount by which the length of the infected file increases), the displacement of the hexadecimal pattern within the virus and the hexadecimal pattern itself. Minor variations of viruses will be restricted to the second part of the table. The hexadecimal pattern can be used to detect the presence of the virus by using any pattern searching software such as the *Norton Utilities*.

We no longer support the idea of using the infective length of a Parasitic virus as an alias. We feel that to continue to do so would be to condone a bad practice which can cause confusion. Those who require this information will now find the infective length in the programmer's section of the table.

KNOWN APPLE MACINTOSH VIRUSES

David Ferbrache

The following is a list of the **known** viruses affecting Apple Macintosh computers. Each entry includes the name (and aliases) for the virus; a short description of symptoms; together with the characteristic resources or byte sequences which can be used to detect the virus' presence.

Name	Family	Description
nVIR A	nVIR	When an infected application is executed nVIR A infects the system file (adding an INIT 32 resource), thereafter any reboot will cause the virus to become resident in memory, after which any application launched will become infected. There is a delay period before the virus will begin to announce its presence. This announcement is made once every 16 reboots or 8 infected application launches by either beeping or using Macintalk to say "Don't Panic".
nVIR B	nVIR	Similar to nVIR A but does not utilise Macintalk if installed. Beeps once every 8 reboots or 4 application launches.
Hpat	nVIR	Identical to nVIR B but for resource details.
AIDS	nVIR	Identical to nVIR B but for resource details.
MEV#	nVIR	Identical to nVIR B but for resource details. Other members of this family are reported to randomly delete files from the system folder.
Peace	Peace	Also known as the Drew or MacMag virus. The virus does not infect applications but only propagates to system files present on hard or floppy disks. The virus was designed to display a message of world peace on March 2nd 1988, and then delete itself from the system file.
Scores	Scores	When an infected application is executed Scores will infect the system file, note pad and scrapbook files; the icons for the last two are changed to a generic document icon. In addition two invisible files are created, named Scores and Desktop. Following a boot from the infected system file the virus is loaded into memory. Two days after infection of the system file the virus will begin to infect any application run within 2 to 3 minutes of its launch. After four days any applications run with "ERIC" or "VULT" resources will cause a system bomb (ID = 12) after 25 minutes. After seven days any application with "VULT" resources will find its disk writes returning system errors after 15 minutes of runtime.
INIT 29	INIT 29	When an infected application is run INIT 29 will infect the system file and patch the open resource file trap. Any action which opens the resource fork of a file will cause the fork to be infected. Note that this virus does not require an application to be run for it to be infected. Only infected system files or applications will spread the virus although other files may be infected. This virus will attempt to infect any newly inserted disk causing the message "the disk needs minor repairs" if it is write protected. Sporadic printing problems may also be encountered.
ANTI	ANTI	This is the first virus for the Mac which does not add new resources on infection, the virus instead appends its code to the CODE 1 resource of the infected application. When an infected application is run the virus will install itself in the system heap, and thereafter infect any application which is launched or has its resource fork opened. Unlike other Mac viruses it does not infect the system file, and thus will only become active in memory when an infected application is run. Anti does not spread under multifinder. The virus is also designed to execute automatically a code block on floppy disks which carry a special signature word.
Dukakis	Hypertext	A virus written in hypertalk which when activated will install itself in the home stack displaying the message "greetings from the hyperavenger... dukakis for President ... Peace on Earth and have a nice day". The virus will then propagate to each stack used, displaying its greeting at three week intervals.

Resources added on infection: resource name, number and length in bytes *n* represents the number of the highest allocated code resource:

Virus	System file			Application			Common to both		
nVIR A	INIT	32	366b	CODE	256	372b	nVIR	1	378b
	nVIR	0	2b	nVIR	2	8b	nVIR	6	868b
	nVIR	4	372b	nVIR	3	366b	nVIR	7	1562b
	nVIR	5	8b	-			-		
nVIR B	INIT	32	416b	CODE	256	422b	nVIR	1	428b
	nVIR	0	2b	nVIR	2	8b	nVIR	6	66b
	nVIR	4	422b	nVIR	3	416b	nVIR	7	2106b
	nVIR	5	8b	-			-		
Hpat	INIT	32	416b	CODE	255	422b	Hpat	1	428b
	Hpat	0	2b	Hpat	2	8b	Hpat	6	66b
	Hpat	4	422b	Hpat	3	416b	Hpat	7	2106b
	Hpat	5	8b	-			-		
Scores	INIT	6	772b	CODE	*n*+2	7026b	-		
	INIT	10	1020b	-			-		
	INIT	17	480b	-			-		
	atpl	128	2410b	-			-		
	DATA	400	7026b	-			-		
INIT 29	INIT	29	712b	CODE	*n*+1	712b	-		
Peace	INIT	6	1832b "RR"	-			-		
Anti		-		CODE 1 extended by 1344b			-		

MEV# and AIDS, similar resources to nVIR B but of resource types MEV# and AIDS in place of nVIR.

Characteristic byte sequences: (from Virus detective Ver 3.0.1)

nVIR resource size < 800b, 2F3A .. 15 bytes .. 00 .. 12 bytes .. 80

Anti in CODE 1 resource last 1344 bytes, 060CA9 .. 6 bytes .. 43E9

LETTER FROM AMERICA

The 'Killer Virus' Strikes

There have been a number of reports recently of a so-called 'Killer Virus' attacking the machines of some correspondents. A killer virus is one that is designed to evade monitor-type anti-virus programs. Apparently, the difference between a 'normal' virus and a 'killer' virus can be fewer than five bytes.

What can you do to protect your system? The first thought might be to use a virus scan program which scans all the files on your hard disk and looks for specific viruses. Note the word "specific". It's a key word, and makes these virus scan programs useless. When a virus infects a program, it leaves a characteristic identification area, easily found by looking for it in each file of your disk. However, until a virus has been isolated and studied its characteristics are unknown. Therefore, scan programs can only be used to search for **known** viruses.

The other alternative, and the only one that will work, is to use a checksum or CRC'er program; one that generates a unique signature for each executable file on your disk, then checks whether examined programs have changed since the signature was generated. If so, the program may be infected. It may also have been updated or might be a program whose installation options are stored within the executable image itself - such a program will tell you that an executable has changed, but can not tell you why.

A checksum program can have two parts. The first part simply scans the disk and generates the checksums, telling you if any listed program has changed. The second part is a small TSR that examines each program before it is loaded and determines whether the checksum on that program has changed.

Looking to the future, what about a killer virus that specifically resets the current set of interrupt service routine addresses to point to their original setting, as if no TSR exists at all? This effectively removes the protection offered by many anti-virus programs. Your only line of defence will be a checksum of the files immediately upon booting-up on a clean, write-protected copy of your operating system. Checksumming entire files is time consuming (one commercial anti-virus package with this capability suggests taking a coffee break for the 45 minutes it needs to checksum the files completely!). Is there an alternative?

Yes - but it might be a risky one. The current crop of viruses all modify the first few bytes of an executable to cause them to jump to the actual virus code usually installed later in the program.

Checking just those first few bytes of program would go a long way towards ensuring the integrity of a file. So would checking the length of a file; almost every known virus adds a few bytes to the length of a file. But this need not be the case. A virus could, for example, simply look for what appears to be a legitimate exit-to-operating system call and tag onto that. Alternatively it could look for a program's stack space (usually initialised to nulls) and infect through those vectors. Therefore we're back to searching the entire file and generating a file-wide checksum.

Checksumming, in the literal sense of summing up all the bytes together, is easy to evade. The virus writer need only generate data in addition to their code to produce an effective zero on the checksum. No simple checksum program will notice the change.

A CRC, using the widely published CRC routines, would be almost as ineffective.

Using a sophisticated algorithm may prove time consuming but will be far more secure. A possible practical solution is to use two checksum programs, each with a different checksumming algorithm. That way the virus writer doesn't know which programs are in use. Two separate programs will provide more security than any individual program can. Alternatively, one can use a strong cryptographicly-based algorithm with two different initialisation values chosen at random.

Ross M. Greenberg

The September edition of the Virus Bulletin will feature an article analysing the strengths and weaknesses of various integrity checking methods which are used in anti-virus software.

LETTER FROM EUROPE

Shrink-Wrapped Viruses

There have been a number of recent incidents of computer virus infection caused by software supplied by bona fide manufacturers and retailers in West Germany. The cases are reported here anonymously because it is difficult to prove that a particular supplier's software was the exclusive carrier of a virus.

In 1988 a graphics software package was introduced by an international software company. Designed for Macintosh PCs, the clients who tested it complained that data stored on hard-disks had been corrupted and files deleted. A virus also infected the compiler system of a software supplier in Dusseldorf. All software designed for Commodore systems supplied over a period of nearly three months was infected. These cases were examined by German security authorities who confirmed that in both instances computer virus programs caused the damage.

Certain MS-DOS commands may cause physical damage. Since Ralf Burger published his book '*Das Grosse Computerviren-Buch*' in 1987, everyone, even those with minimal programming knowledge, have been able to create a functioning computer virus. Among other damaging functions, Burger described in detail how to destroy a hard-disk.

A test release of a well-known database system caused this particular damage to a large number of hard-disks in Germany last summer. I noted a number of similarities in case descriptions from PC specialists at different infected sites. All the victims had tested the new database release prior to suffering hard-disk damage.

In conclusion, software whether copied (illegally or public domain) or sold officially by a bona fide supplier may include undesired functions. It is advisable to inspect all new software in isolation before installation on the system.

Hans Gliss

TECHNICAL REVIEW

Joe Hirst

Virus Bulletin has not received permission to reproduce this article on CD from the author. Readers can obtain a paper copy of the original issue directly from *VB*.

VIRUS DISSECTION

Joe Hirst

Virus Bulletin has not received permission to reproduce this article on CD from the author. Readers can obtain a paper copy of the original issue directly from *VB*.

TECHNICAL REVIEW

Dr. Keith Jackson

PC Immunise

PC Immunise comes as three programs on a single 5.25 inch floppy disk with a very thin (eight pages of A5) manual. Of the three programs, one provides a demonstration, another provides help facilities, and the final one is PC Immunise itself.

PC Immunise helps to detect unsolicited changes by spotting:

1. changes to system software and the operating system
2. arrival of new invisible files
3. creation of files and directories
4. deletion of files and directories
5. amendments to files

The user can choose one of three detection levels, ranging from the **High level** of detection which covers all five entries in the above list, down to a **Low level** of detection which only covers the first point in the list.

PC Immunise uses a checksumming process to detect changes to a file, and keeps track of which files should be in particular directories on the disk. It will spot changes whether they are caused by a virus or by any other means. There are many such checksum programs on sale, and the two distinguishing factors are the algorithm used to calculate the checksums, and speed of execution.

PC Immunise is fairly easy to use. The same program with different command line parameters is used to initiate the setup process, recalculate the checksums, or test that the checksums are correct. The manual contains a good (but brief) discussion about how frequently a user may wish to test his system.

The main problem with using PC Immunise is that it is extremely slow. This comment applies to both the speed of execution, and the speed at which the screen is updated. When execution commenced it took 15 seconds before anything happened on screen, and then a further 50 seconds before PC Immunise requested input of the user identification password.

To complete all of the stages of PC Immunise setup at the High level of detection takes 1 minute 55 seconds using a 3.5 inch 720 Kbyte disk which only contains MS-DOS and the PC Immunise files. This setup time rises to 2 minutes 7 seconds when over 600 Kbytes of the disk are occupied by files. No matter how full the disk was, and no matter what level of protection was chosen, the time to check the floppy disk was always at least 57 seconds (and never more than 1 minute 13 seconds).

Now I fully appreciate that these times can be reduced by using a faster computer, but they never reach the stage where the user does not notice the long checking time.

As evidence of this I tried PC Immunise on a Compaq SLT/286 which has a 12MHz 80286 processor. Execution from floppy disk still takes 24 seconds during setup to reach the stage of requesting input of the user identification password, and checking a floppy disk still takes 39 seconds. The equivalent figures on the Compaq hard disk are 7 seconds and 29 seconds. I think that this hard disk setup time is acceptable, but almost 30 seconds checking time is probably more than most users will stomach every time their computer is booted.

I tried out PC Immunise with various file alterations, and it is certainly capable of spotting alterations to a file, creation of a new file, or deletion of a file. A short report is produced on screen for each problem detected.

Data required by PC Immunise is stored on disk in a hidden file held in encrypted form. The file is called IM UNISE.DAT (notice the space between M and U in the middle of the file name). This space makes it impossible to enter the file name in a DOS command, even if wild- card characters are used. Just to make malicious intervention even harder, the file has Read-only, Hidden, and System attributes. Utility programs can change these attribute settings, but such methods certainly makes malicious intervention more difficult.

Having dug around inside this file, I can confirm that the password required to identify the correct user is not available in plain text form within the file, but curiously there are a dozen repetitions of the text “+++ Curiosity killed the cat” at the start of the file. Someone’s idea of a joke ?

Details of the algorithm used to calculate checksums are not disclosed by the developer, which prevents any comment on the cryptographic strength of the algorithm. To prevent reverse engineering by a particularly clever virus, such an algorithm **must** be cryptographically strong. If it is not, it may be possible to deduce the algorithm from inspecting checksums and/or files. As I don’t know what the algorithm is, and cannot deduce it from PC Immunise operation, I cannot comment on its strength. You are at the mercy of the developer’s cryptographic expertise on this point.

There is a balance that must be struck between cryptographic strength (which is essential), and speed of execution (which is extremely desirable). Given the figures quoted above, PC Immunise will struggle to pass any speed tests that a user may care to devise.

There are many loose edges to PC Immunise :

1. If PC Immunise is looking for a floppy disk, and you have forgotten to insert a disk, the DOS message “Retry, Abort, Ignore ...” comes through on to the PC Immunise screen. The program should capture this error and take appropriate action within the

bounds of the screen layout.

2. In the demonstration program, and PC Immunise itself there is no way to terminate execution from the keyboard. This was confirmed by the developer. What it means is that apart from rebooting the computer, the only way to get out of a PC Immunise program is to struggle on to the bitter end. Take note of my comments above about speed of execution to realise how frustrating this is.

3. When passwords are first entered, during setup, they are visible on the screen. A password should **NEVER** be visible on the screen. Under any circumstances.

4. If a disk is nearly full (say only 5k left, when at least 8k is required by PC Immunise), the error:

"Unable to access IMMUNISE Data"

appears. This is obscure to say the least. A message saying "disk full" would be more helpful, but that's not all. As there is no way to escape from a PC Immunise program you have to reboot the computer to exit from this stage of the program. Not very helpful.

5. PC Immunise will leave hidden data files behind on a disk if you ever cease using it. There is no option to uninstall the package. Such files are difficult, if not impossible, for the average user to delete.

I'm unhappy about the tenor of the manual's content and I also heartily dislike the disclaimer in the manual which states that the vendor "specifically disclaims any implied warranties or merchantability or fitness for any particular purpose". Such sweeping disclaimers make one doubt the motives behind the statement, and it is probably not legally valid anyway. Goods must be fit for their stated purpose, and if they are not, a refund of the purchase price can be claimed. I do not believe that computer software can claim exemption from such laws by the mere inclusion of legal gobbledygook.

The information in the manual is in the main correct, it's the bits that are left unsaid, and the extremely condensed layout (it's only eight pages long) that jars most . It must be possible to do better than this. The manual writing process seems to have been affected by 'gremlins', as the three paragraphs near the end of section 13 are repeated.

The on-line help provided is far better than the manual, and I would be tempted to use this in preference to the manual.

My conclusions on PC Immunise are very straightforward. It does detect changes to files and/or the operating system, but does so only slowly. Once any of the PC Immunise programs are operating, you have no choice but to struggle on to the end, as there is no way of prematurely terminating execution. I can't comment on whether the algorithm used by PC Immunise to calculate checksums is cryptographically strong (as it should be), because the developer does not release details.

At under £20, PC Immunise is very cheap, but it needs further development work.

Technical Details

Developer: S A Software, 28 Denbigh Road, London, W13 8NH, England (Tel. 01 998 2351)

Vendor: Artronic Ltd., 1-3 Haywra Crescent, Harrogate, North Yorkshire HG1 5BG, England (Tel. 0423 525325)

Availability: IBM PC/XT/AT, PS/2, or any close compatible running MS-DOS or PC-DOS

Version evaluated: v1.20

Price: £19.95, one-off price

Hardware used :

a) ITT XTRA (a PC compatible) with a 4.77MHz 8088 processor, one 3.5 inch (720K) drive, two 5.25 inch (360K) drives, and a 30 Mbyte Western Digital Hardcard, running under MS-DOS v3.30

b) Compaq SLT/286 (a battery powered laptop portable) with a 12MHz 80286 processor, one 3.5 inch (720K) drive and a 20 Mbyte internal hard disk, running under MS-DOS v3.30.

CONFERENCE REPORT

Edward Wilding

Computer Viruses, Marriott Hotel, London, 29th June 1989.

"Those of you who haven't been hit yet...just be patient!" The words of Robert Jacobson, first speaker at this one day seminar organised by IBC Technical Services, who painted a demoralising picture of virus propagation in the United States which he likened to a 'growth industry'. He talked of the destruction wraught in Silicon Valley on Friday 13th January 1989, of the Internet worm and of 'second generation' viruses which he described as ''fiendishly clever''. Future virus attacks, predicts Jacobson, will occur on AS/400 and small VAX systems.

Mark Gibbs from Novell quashed the theory of safe or 'benign' viruses - the programs can have very different effects as operating systems evolve and what appears harmless under DOS Version 3.1 may prove destructive running on DOS Version 4. The recent appearance of pernicious variants of n-VIR proved that seemingly harmless viruses can be transformed if they fall into the wrong hands. Ensuring software reliability was becoming ever more difficult - even IBM, he said, had shipped a virus from their duplication facility in Holland. Gibbs proposed a management solution to the virus threat; "Fire anyone who introduces new software to a system without authorisation".

UK expert on computer law Alistair Kelman, guided the audience gently through the legal position relating to computer viruses. Information is not regarded as property in UK law and a prosecution under the Criminal Damage Act of 1977 against the virus writer could only succeed if it were proved that damage to 'property of a tangible nature' had occurred. Defining such 'property' was a complex task compounded by the fact that a case of harmful intent or recklessness had to be proved against the accused. Kelman also explored the minefield of civil liability and negligence. It became clear that UK law has not even begun to address computer vandalism.

The 'siesta hour' following lunch was enlivened by an on-screen display of computer viruses conducted by Dr. Jan Hruska. He demonstrated Cascade, showing how the virus added 1701 bytes to the infected file and caused the displayed letters to fall to the bottom of the screen and a simulation of the Fu Manchu virus. Hruska described in detail the manner in which viruses can infect a computer and the various software available to combat this process. He also referred to 'dirty PCs' - standalone computers designated exclusively for gameplaying and untested software as a possible first line of defence.

Dennis D Steinauer (National Institute of Standards & Technology, USA) discussed the lessons learned in the aftermath of the Internet worm and stressed the need for a coordinated response to emergencies and for cooperation between specialists in specific operating environments ('constituencies' in NIST terminology). The Computer Emergency Response Team or CERT is one such initiative for crisis management on the US Arpanet network.

''Prevention is better than cure'' was the opening message of David Frost's presentation. He talked of the common computer viruses at large, including Brain, Vienna, Cascade and Jerusalem. Frost emphasised the need to keep an inventory of write-protected trusted software to assist recovery from a viral infection.

The final speaker, Paul Wiltshire from Deloitte Haskins & Sells, warned that European organisations had approximately six months to prepare for the impending virus onslaught. Wiltshire favours using numbers (as opposed to names) to describe computer viruses. Tackling virus families or variants could speed the development of countermeasures and recovery in the event of an attack. Viruses, he said, would soon become a mainframe problem with the portability and transfer of programs posing a potential threat to systems such as DEC and Unysis. He also proposed the selective use of 'clean PCs' - the isolation of certain sensitive machines from all sources of infection. Finally, education and training involved explaining the reasons behind procedures rather than the provision of endless checklists of 'dos and don'ts'.

The seminar concluded with a panel session. There was agreement that computer viruses were becoming more numerous, more destructive and more insidious but disunity about what should be done in the face of the impending crisis. Perhaps the most reassuring statement came from Paul Wiltshire; "Don't panic, we will learn to manage this problem".

EVENTS

Galactic Hacker Party, Paradiso, Amsterdam, The Netherlands. A dubious three-day event commenced on August 2, 1989. Presentations by Chaos Computer Club and other members of the opposition. Tel +31 20 6001480 or write to Rop Gongrijp, PO Box 22953, 1100 D1 Amsterdam, The Netherlands.

Datapro is holding a one-day seminar on **Logic Bombs, Trojan Horses and Computer Viruses**. It takes place in London on 12 September 1989. Details from Rosemary White at Datapro, UK, Tel 0628 773277.

S&S Consulting Group is holding two one-day 'strategic' seminars on the **Virus Threat**. They take place on 13 September and 16 November 1989 at Rickmansworth, Herts, UK. Details from S&S Enterprises, Tel 0494 791900.

The IBM PC User Group is holding a two-day event on **Security for PCs and Networks**. The event takes place at the Royal Aeronautical Society, London, on 19 and 20 September. Details from Gordon Condrup on Tel 01 863 1191.

Sophos Ltd continue a series of **Virus Workshops**. The next available workshops are on 25 September, 24 October 1989 and 21 November 1989 and are held in London, Edinburgh and Oxford respectively. Further details from Karen Richardson at Sophos, UK, on Tel 0844 292392.

Compsec '89 in conjunction with the EDP Auditors Annual Conference. The largest computer security conference in the UK includes a three hour special presentation on the virus threat. The event takes place at the QE II Centre, London, from 11-13 October, 1989. Details from Penny Moon, Elsevier Seminars, UK, Tel 0865 512242.

The **Annual brief on Secure Systems.** This annual report on global computer security developments takes place on 29-30 November, 1989 at the Hague, the Netherlands. Details from Peter Hoogenboom, The Netherlands, Tel +31 3403 79597.

VIRUS BULLETIN

Subscription price for 1 year (12 issues) including delivery:

US$ for USA (first class airmail) $350, Rest of the World (first class airmail) £195

Editorial enquiries, subscription enquiries, orders and payments:

Virus Bulletin Ltd, Haddenham, Aylesbury, HP17 8JD, England

Tel (0844) 290396, International Tel (+44) 844 290396
Fax (0844) 291409, International Fax (+44) 844 291409

US subscriptions only:

June Jordan, Virus Bulletin, PO Box 875, 454 Main Street, Ridgefield, CT 06877

Tel 203 431 8720, Fax 203 431 8165