November 1989 ISSN 0956-9979

VIRUS BULLETIN

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

CONTENTS

EDITORIAL

Friday 13th

The Royal National Institute for the Blind was the first UK organisation to report a virus attack on October 13th. Their machines were infected with the Jerusalem virus and it was at first feared that a substantial amount of programs had been irretrievably lost. Dr. Alan Solomon who took charge of the clear up operation at the RNIB's London offices was later able to confirm that this was no the case. However, one of the fears voiced by a spokesman for the RNIB was that application disks which are regularly distributed to a large number if visually handicapped people may have been infected.

Two quick observations. First, the RNIB incidents proves yet again the wholly indiscriminate nature of computer virus attacks. Some reports suggested that the attack was intentional - such reports emanated due to ignorance by some journalist as to the nature of computer virus infection. Virus writers want to cause inconvenience or wanton destruction, it is of no concern to them as to the nature of the programs and/or data which is lost. Second, it is interesting that a charitable organisation spoke openly about the problem, while corporates and business victims (were there any?) remained silent.

Datacrime

In July of this year *Virus Bulletin* played a central role in warning about the Datacrime virus. It gradually became apparent that Datacrime was not as widespread as we had first believed. Very few incidents of Datacrime infection have actually been reported to date and it appears that the propagation of this particular virus and its variants will take some time. A Catch-22 dilemma exists: to warn about or to understate a potentially serious problem? When dealing the computer viruses we have learned that predictions are probably best left unstated.

Readers should note that the information about the Datacrime II computer virus which appeared on page 4 and 9 of last month's edition of *Virus Bulletin* is incorrect. Correct details appear on page 12 of this edition.

The Parker Prediction

One man who is not afraid to predict the future of computer viruses is Donn Parker, the US criminologist who works at SRI - the former Standford Research Institute in California. Parker visited London in October and predicted the end of the computer virus phenomenon.

He regards computer viruses as a 'crimoid' - a word which seems to mean the latest in a succession of security problems which have been 'hyped' by the press. Parker's previous crimoids include phone-phreaking, salami-fraud, hacking and wire-tapping. Parker believes that 'hype' can be beneficial in bringing security issues to management's attention and that news media coverage reduces the appeal of perpetrating 'crimoid' acts. Parker, who has spent 20 years researching hacking and computer security issues, believes that virus abuse will also decline because of the high work factor involved in writing the programs.

It is certainly true that computer viruses are not longer a novelty. There is nothing particularly amazing about writing replicating code - it has, after all, been done before. The challenge of writing such programs has probably diminished. However, the deviant is likely to persist with the use of viruses because MS-DOS (in particular) is so widely used and so vulnerable to virus attack. Also, once viral code is in circulation it can undergo any number of alterations. The process requires relatively little time and effort on the part of the perpetrator. Finally, articles in magazines such as *Reality Hackers* about 'hunter/killer' viruses, 'salami' viruses, 'total destruction' viruses and even viruses designed to cause hardware damage show that a number of unnerving ideas are spreading.

Disk-Killer

This virus which infects IBM PCs and clones was first reported in the UK in mid October. According to *PC Business World* the virus originated in the United States and displays the screen message "Disk Killer Version 1.00 by Ogre Software, April 1, 1989. Do not turn off the power or remove the diskett while processing!". The virus also destroys the hard-disk.

Virus Bulletin will distribute details for programmers and further information to all subscribers as soon as possible.

Worm Programs

In this month's edition there is a short article about worm programs, including a brief analysis of the DECnet worm which struck the NASA Space Physics Astronomy Network last month. This reflects our intention to expand our coverage to include discussion and analysis of a variety of malicious programs in a number of operating environments. More detailed articles about both the Internet Worm and last month's DECnet incident will appear in a future edition of the bulletin.

WORM PROGRAM

David Ferbrache

The Internet Worm One Year On

On November 2nd 1988 a worm struck the US DARPA Internet computer network. A worm is similar to a virus in that it is a replicating code segment but unlike a virus the worm does not incorporate its code into a host program, but reproduces directly.

The Internet worm was allegedly released by Robert T. Morris, a Cornell University student, at 5.02pm EST. The worm replicated by exploiting a number of bugs in the UNIX operating system, including a bug in sendmail (a common Unix email program) and in fingerd (a process enabling users to obtain details concerning people logged into a system). By 9pm Stanford University was infected, by 9.30pm Massachusetts Institutes of Technology, by 10.45pm the University of Maryland and by 11pm the University of California at Berkeley. The NASA Research Institute at Ames and the Lawrence Livermore National Laboratory were also hit.

Throughout the night university specialists analysed the worm's method of replication, resulting in a bug fix posted at 6am on Thursday by the University of Berkeley to correct the *sendmail* bug.

At 11.30am the connection between Milnet (an unclassified military research network) and Internet was severed by the Defense Communications Agency. This link remained inoperative until 11am on Friday.

The *fingerd* bug was identified at 7.20pm that day. The worm became news at 11pm on both TV and radio. On November 4th New York Times ran the headline "Virus [sic] in military computers disrupts systems nationwide", "Largest assault ever on the nation's systems".

After the worm had been disassembled and decompiled, a number of derogatory comments were made about the author's coding style. One observation was that the fast encryption routines used by the worm to search for possible user passwords were well written and seemed to have come from a separate source.

In the aftermath of the worm, measures have been taken to improve both network and UNIX security and formal procedures for dealing with worms have been established. The Computer Emergency Response Team (CERT) now provides a 24-hour co-ordination centre for security related incident reporting. UNIX email security lists have been expanded, and a wide rage of bug fixes are available from the University of California at Berkeley as part of a review of UNIX security.

The UK was unaffected by the Internet worm due to the loosely coupled nature of mail bridges between our principal academic network (JANET) and the US.

NASA SPAN Struck Again

On October 16th 1989 the NASA Space Physics Astronomy Network (SPAN) was struck by a worm.

The SPAN network was also hit by a worm launched on December 23rd 1988 which bid each user a Merry Christmas, and issued them a stern instruction to "stop computing and have a good time at home!!!!". The current worm is more sinister in that it incorporates code to mail passwords back to its originator, and irritates users both through text displayed at login time, and by issuing random messages.

The new worm exploits the openness of many DECnet hosts and the poor choice of system and user passwords. The worm propagates on any network using DECnet protocols rather than the TCP/IP protocols used by the Internet worm. When a system is infected the worm will:

1. Change the default DECNET password to a random string.

2. Mail the password used to access the system to a specified user.

3. Change its process name to "NETW" followed by random digits.

4. Change the system login banner message to "WORMS AGAINST NUCLEAR KILLERS" followed by abbreviated form of this message in graphics, followed by "You talk of time of peace for all, and then prepare for war".

5. Disable mail to the system account and modify the login command to make it appear as if files have been deleted.

6. Attempt to change the FIELD account password and allow logins from any host.

7. Phone users randomly on selected remote systems (writing messages to screen) for irritation.

8. Attempt to access a remote system using the user list found with passwords which match the account name or are blank.

9. Copy itself to an account found above (preferably with system permissions) and propagate further.

Numerous copies of the worm exist. It is possible that it may appear on other DECnet systems isolated from SPAN. Details of this worm, its operation and suggested fixes are available from the email address <cert@sei.cmu.edu>, or by telephone to Tel USA 412-268-7090.

KNOWN IBM PC VIRUSES

The following is a list of the known viruses affecting IMB PCs and compatibles, including XTs, ATs and PS/2s. The list consists of two parts. The first part of the list gives aliases and brief descriptions, and this also includes a section on reported viruses (which may be completely inaccurate). The second part includes the infective length (the amount by which the length of an infected file has increased), the hexadecimal pattern to use for detecting the virus, and the offset of this pattern within the virus. Viruses referred to in other publications by number almost always refer to the infective length. The hexadecimal pattern can be used to detect the presence of the virus by using the "search" routine of disk utility programs such as *The Norton Utilities*.

Short descriptions of Syslock & Dark Avenger have had to be postponed. Vacsina is still awaiting disassembly, as are MIXI, Typo and the Dbase virus.

MANAGEMENT ISSUES

Insurance: Lloyds systems Perils Policy Addresses Virus Threat

In December of last year an insurance scheme known as the Lloyds Systems Perils Policy was launched. The 'Perils Policy' contained a number if innovative features designed to revolutionise the insurance of computers and telecommunications facilities. One such feature was the claim that the policy included insurance cover for businesses whose computers became infected with computer viruses. Virus Bulletin recently visited the London offices of Data Integrity plc, the consultancy charged with pre-insurance risk assessment to discuss the insurance industry's gradual awakening to new computer threats.

"Computer technology" explains Frank Austin "is the major insurance question for the 1990s - business computer-dependency is causing something of an upheaval within the highly conservative insurance industry. It is slowly becoming apparent that traditional insurance policies are simply not suited to the business EDP environment". Austin is the man responsible for drafting the Lloyds Systems Perils Policy, a computer-related insurance policy which places emphasis on consequential loss - or business interruption as it is also called.

Traditionally, computers have been regarded in much the same way as other forms of office equipment. If hardware was flooded, bombed, caught fire or suffered from any other disaster it would be replaced or repaired by the insurance company. Such insurance policies were adaptations of existing policies designed to cover technical equipment or industrial plant. In many instances this has been done by adding the hardware to the physical damage fire policy.

This type of insurance cover is inadequate for companies heavily reliant on the continuing operation of their data processing and/or telecommunications equipment. As Austin explains "Its no good having equipment replaced if in the meantime your business has collapsed. For instance, one of the banks we recently spoke to admitted that one of their 'real-time' systems was so critical to their operation that its loss would entail a collapse of the business within 72 hours".

In consequential loss (of 'con-loss') policies it is the continued operation of the business and not just the computers which is being insured. Should a computer or telecomms disaster occur, the underwriters will pay the afflicted company the revenues lost and/or costs incurred die to its inability to function properly. Such costs can include loss of earnings, failure to meet contractual obligations, emergency expenditure for off-site facilities and the like. This payment is in addition to reparation of damage to equipment, data and software.

"The policy" says Austin "recognises that insurance cover should reflect realistic risks faced by the business client. Computer-dependent companies should be able to place their most critical operations at the very heart of their insurance cover". However, as would be expected the policy places far greater emphasis on company controls and risk management than more traditional forms of computer insurance. The underwriters for the policy require assurance that all reasonable precautions have been taken to minimise exposure to computer threats and to provide suitable disaster recovery plans. A pre-condition of the Perils Policy is that a survey is conducted to evaluate the potential client's risks.

Data Integrity plc are responsible for conducting risk assessment for prospective clients and furnish a report to the underwriters before insurance cover is agreed. Steve Mills of Data Integrity described the risk assessment process: "We look not only at the technical environment to ascertain the critical systems and how best to protect them but also at the financial impact resulting from the loss of these systems. This, of course, means speaking not only to DP professionals, but also accountants, financial and senior management. By examining documentation, interviewing key personnel and site inspection a report is compiled which identifies security weaknesses with recommendations on correcting them. Compliance with these recommendations will obviously lower the client's insurance premium but ultimately the underwriters will decide whether or not the level of risk is acceptable". Lloyds Underwriters may also require Data Integrity to conduct re-survey checks to ensure that a client is maintaining the agreed procedural and technical security standards. "We would be particularly anxious" explains Austin "to review our assessment in the event of evolving DP environment where major upheaval in systems and operations was envisaged or taking place".

Both Austin and Mills are at pains to emphasis the importance of striking the correct balance between security and business efficiency. Austin explains "If security becomes so overbearing that it impairs the prosper functioning of the business then it has, obviously, become a self-defeating exercise". "Furthermore" adds Mills "you cannot predict or assess every risk".

At the moment the Perils Policy offers a maximum insurance of £20 million for financial loss in the event of 'downtime'. This is planned to increase as custom develops. Mills explained some of the problems in launching an insurance policy which contains an unusually high technical content; "Brokers, underwriters and, indeed, senior management are often wary of change. Any policy which requires a certain level of technical expertise to understand and implement is bound to meet some resistance. It took three years for the Computer Risk Insurance Policy [now an industry standard] to be accepted. We're pleased that so much interest is being shown at this relatively early stage".

The Perils Policy is claimed as the first to provide insurance cover against computer virus attack. Steve Mills explains, "In the case of viruses we would expect strong rules prohibiting the use of unauthorised software, regular and documented backups, and strict controls on the passage of software both internally and externally. Obviously, different organisations will have different levels of exposure. A company using a microcomputer LAN or WAN to conduct critical business applications would be expected to install more stringent anti-virus measures than another client using stand-alones PCs for less sensitive operations". In certain instances Data Integrity might, for instance, expect mandatory use of anti-virus and integrity checking software.

Viruses are among a number if threats which traditional computer insurance policies have ignored. Data corruption and other such hazards have not previously featured in insurance policies because data is so difficult to quantify in purely financial terms. Austin claims that the Perils Policy is the first to address such problem areas as Trojan, logic bombs, time bombs and viruses. The company does not define computer viruses strictly in terms of microcomputer use, their risk assessment methodology aims to establish both the likelihood and impact of a virus attack in a multitude of operating environments including mainframe and minicomputer. The policy would cover for the period of 'downtime' resulting from a virus attach including both the costs incurred in restoring the system and the estimated loss to the client. In general terms, Austin admits that insurance premiums will rise or fall in relation to the estimated level of threat which computer viruses and other threats pose. Not only must destructiveness be accounted for (as in such viruses as Datacrime and Disk-Killer) but also infectiousness and the extent of computer virus distribution. Moreover, where a prospective client had suffered a previous virus attack or a succession of such attacks, the risk assessment would included a scrupulous process of software validation and an examination to find out if procedures were being overlooked or not adhered to.

Data Integrity stress that the Perils Policy was not primarily designed as a virus cover and includes a very large element of standard cover. Other threats which the policy aims to address include the loss of telecommunications, business information facilities, electricity supply, software and data faults, and data/program destruction and corruption caused by hackers. The policy is modular and can be adapted to interrelate with an organisation's existing insurance in order to provide more comprehensive cover. It is principally aimed at the banking and finance community and Data Integrity hope to conclude the first policy by the end of this year. There are also plans to prepare similar policies tailored for manufacturing industry and retail wholesale businesses to provide insurance cover for, among other things, EFTPO transactions.

In recent years there has been a noticeable increase in computer security awareness within the industrial and business communities. As a result calls are being made for realistic insurance policies to cover computing and communication facilities. The insurance industry is now awakening to customer requirements and we can assume that the Perils Policy will be just the first of a series of new computer-related insurance initiatives.

Lloyds Systems Perils Policy Broker: Jardines Insurance Brokers International Ltd, Jardine House, 6 Crutched Friars, London EC3N 2HT, UK, Tel 01 528 4690

Data Integrity plc, 31 Harley Street, London WIN 1DA, UK, Tel 01636 1971

EVALUATION

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*.

EVALUATION

David Ferbrache

Software Tools to Combat Macintosh Viral Infection

Virus Bulletin is carrying out a systematic review of all Macintosh anti-viral software (both commercial and public domain) to establish its effectiveness in combating known and possible future viruses. This edition reviews the Symantec anti-virus product 1.0, Virex 2.1, Dininfectant 1.2, Virus Detective 3.0.1 and VirusRx 1.4a2.

The review consists of tests against a range of viruses including known viruses like Anti, INIT 29, nVIR a/b/clones, Scores, Peace RR/DR, possible mutations like new nVIR and Scores clones, cross breeds of known viruses and inhibitor resources.

The new addition this month is the Virex product from HJC Software version 2.1. It dealt successfully with the majority of the known Mac viruses including the newer nVIR B clones such as MEV # and nFLU.

The product fails to detect the Peace virus (in either strain) and does not deal with possible future nVIR B clones. The latter can be explained by a dependence on resource name and id checks rather than on code signatures. Virex does however deal sensibly with the nVIR 10 inhibitor, reporting it as such, rather than as an nVIR resource.

Virus Detective still seems to demonstrate the best detection algorithms and has the added convenience of being configured as a desk accessory with the ability to auto-scan floppy disks under multi-finder. Disinfectant and Virex both proved excellent at removing infections, especially in their abilities to deal with multiple infection instances.

Further to our review of SAM in the previous edition, version 1.1 is now being shipped. This version addresses version 1.0's shortcomings including the inability to detect nFLU and to repair Anti-infected applications.

Sam, Symantec UK, 36 King Street, Maindenhead, SL6 1ES UK, 0628-77634, Commercial, £69

Virex, HJC Software Inc, PO Box 51816, Durham, North Carolina NC 27717, USA, Commercial, $99.95

Disinfectant, John Norstad, Northwestern University, 2129 Sheridan Road, Evanston, Illinois 60208, USA, Shareware, Free

Interferon, MacUser, Userware, PO Box 320, London N21 2NB, UK. Shareware, Charity Donation

VirusRx, MacUser Userware, PO Box 320, London N21 2NB, UK Shareware, Free

Virus Detective, Jeff Shulman, PO Box 521, Ridgefield, CT 06877-0521, USA, Shareware, $25

Product Name	Version Number	Anti	INIT 29	Peace RR	Peace DR	Scores	nVIR A	nVIR B	Hpat	AIDS	MEV#	nFLU
Virex	2.1	R	R	-	-	R	R	R	R	R	R	R
SAM	1.1	R	R	-	R	R	R	R	R	R	R	R
SAM	1.0	D	R	-	R	R	R	R	R	R	R	-
Disinfectant	1.2	R	R	-	R	R	R	R	R	R	R	R
Disinfectant	1.1	R	R	-	R	R	R	R	R	R	R	R
Disinfectant	1.0	R	R	-	R	R	R	R	R	-	-	-
V.Detective	3.1	D	D	D	-	D	D	D	D	D	D	D
V.Detective	3.0	D	D	D	-	D	D	D	D	D	D	D
V.Detective	2.3	-	D	D	-	D	D	D	D	D	D	D
Interferon	3.1	-	-	-	-	D	D	D	D	D	D	D
VirusRx	1.4a2	-	F	-	-	F	F	F	F	F	F	F

Product Name	Version Number	nVIR 10 Inhibit	New nVIR Strain	New Scores Strain	nVIR INIT29	nVir Scores	nVIR Anti
Virex	2.1	-	-	F	R	R	R
SAM	1.1	?	?	?	F	F	F
SAM	1.0	F	-	-	F	F	F
Disinfectant	1.2	-	-	-	R	R	R
Disinfectant	1.1	-	-	-	R	R	R
Disinfectant	1.0	-	-	-	R	R	R
V.Detective	3.1	-	D	D	D	D	D
V.Detective	3.0	-	D	-	D	D	D
V.Detective	2.3	-	D	-	D	D	D
Interferon	3.1	-	D	F	F	F	F
VirusRx	1.4a2	-	F	F	F	F	F

F Virus infection found, cannot disinfect

D virus infection found and infectious code resources removed, cannot restore application to original form.

R Virus infection found, infectious code removed, application repaired

TECHNICAL FEATURE

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*.

PRODUCT REVIEW

Keith Jackson

"FLUSHOT+, Protection Against Malicious Programs"

In the documentation provided with FLUSHOT+, the program is subtitled "A form of protection from Viral and Trojan Programs". I think that this is a succinct decsription of the product which aptly illustrates one of its major advantages: it detects malicious actions by any type of program - not just viruses.

In technical terms, FLUSHOT+ is a memory-resident utility which monitors disk system activity and triggers when 'illegal' operations are detected. It requires the MS-DOS operating system. Any version of MS-DOS can be used, or at leat nor version constraints are stated in the documentation. When FLUSHOT+ is trggered, it asks the user whether a particular action should be allowed or disbarred.

The stated aim of FLUSHOT+, prexent in the message displayed whenever execution commences, is that "Nasty operations will be intercepted". Does it achieve this stated aim?

FLUSHOT+ is provided as a self-extracting archive file. When the program is executed, it extracts data from within itself, and creates the required files on disk. The advantage of such a method of distribution is that the files are compressed into a much smaller form. The distributed file FLUSHOT.EXE is 109 Kbytes long. This expands to 209 Kbytes when the 28 constituent files are extracted - about 50% compression.

FLUSHOT+ states very clearly that it is distributed as shareware, and can only be distributed commercially with the written permission of the author. Non-commercial copying (through bulletin boards etc.) is encouraged. Given that the most common way to obtain a copy of FLUSHOT+ is by lownloading from another computer, the 50% compression described in the previous paragraph is very worthwhile.

The terms Trojan Horse, Virus and Worm are defined in the manual in very light-hearted style. This levity ran a bit thin by the end of the manual. If you think that "slimebucket" is a technical term, then you'll get along fine reading this manual. Mind you, I still chuckle at the idea that eiminating the originator of a virus could be "justifiable homicide".

Assuming that the terms Trojan Horse and virus are familiar ones, I will refer to such programs by the general phrase 'malicious program'.

The name of this product was dhanged to FLUSHOT+ because a previous version (FLUSHOT4) had been converted into a Trojan Horse. Exactly who did this will of course never be known, but the author only released versions 1, 2, and 3 of FLUSHOT. Version 4 was produced from version 3 by persons unknown Trojanising the program provided to help in reading the documentation. Therefore even if you just read the documentation, damage could ensue.

FLUSHOT+ can protect files in many ways. Wildcard specification such as *.COM can be used to sopecify the group (or groups) of files that are to be protected using each of the methods described below. This wildcard specification method is made very powerful by the addition of a file exclusion syntax. Files can be write protected, and/or read protected. Write protection prevents any program writing to a file. Read protection prevents any access to a file until FLUSHOT+ is removed.

Checksums can be calculated (and verified) for any named list of files. The rational behind this is that programs having malicious effects will alter a files content. After all, if this did not happen, then such programs would not be considered malicious. A user must be judicious when using the checksum test, as some programs write their current status back to the executable file.

FLUSHOT+ can provide a checksum test for the boot track of a disk. Some viruses are know to infect this part of the disk, they are particularly dangerous as they can take control before any protection programs sucha s FLUSHOT+ can activate. FLUSHOT+ also protects is memory resident checksum table by checksumming it. As for all ckecksumming methods, the correct checksum must be calculated on a system known to be problem free.

FLUSHOT+ maintains a list of programs that are allowed to become memory resident . Any program becoming memory resident which is not on this list (possibly a virus) will cause FLUSHOT+ to trigger a warning.

In summary, FLUSHOT+ is a memory resident program offering:

a) Write protection for named files b) Read protection for named files c) Memory resident programs constrained

to a stated list d) Checksum verification for named files e) Checksum protection for the boot track on a disk

The user can specify the files for each method of protection differently, and therefore tailor the protection ot their own particular circumstance. The protection scheme is stored in a file called FLUSHOT.DAT. This file is obviously vulnerable to attack by malicious programs, therefore a utility is provided which allows the user to rename FLUSHOT.DAT and store it in any desired subdirectory. As the choice is up to you, presumably a malicious program cannot know where to find the file.

My main complaint about the checksumming process is that there is no description in the documentation of the algorithm used to calculate a checksum. It is vitally important that such an algorithm is cryptographically strong, otherwise a malicious program using an oita of intelligence could alter a program and then make sure that the checksum has not been altere. See "Checksum methods used to deter virus attacks", *Virus Bulletin*, September 1989. FLUSHOT+ does not describe its algorithm, in which case I cannot comment upon its strength.

There are many facilities (too numerous to mention in detail), which can be used to switch off certain features, which may prove annoying. Worthy of individual mention is that FLUSHOT+ indicates that it is protecting a computer by displaying a '+' sign in the top right corner of the screen. If you are about to do some work which will activate FLUSHOT+ (which you know is not harmful), then pressing the ALT key three times temporarily disables FLUSHOT+. The '+' sign then changes to a '-' sign. Pressing Alt three times again, reactivates FLUSHOT+.

Once an event triggers FLUSHOT+, the user can reply Y(es) to allow the operation to proceed, G(o) to allow the operation to be executed until the current program terminates, or press any other key to prevent any action being taken. The user must decide what to do when a FLUSHOT+ trigger is activated. In the end I believe that this is probably the best way to proceed. Hard and fast rules built into software packages are bound to run into problems under certain circumstances. FLUSHOT+ offers plenty of facilities to ensure that the percentage of false triggers is kept very small.

Before I describe the probelms that I encountered with FLUSHOT+, let me state that unless you are interested in viruses per se, then I firmly believe that software which is not specific to particular viruses is the best way to protect your computer against malicious attack. This is for two main reasons. Firstly, detection and prevention methods aimed at specific viruses will have to be updated ad infinitum as the list of know viruses expands. Secondly although viruses are worrying computer users this year, who is to say whay next year's problem will be. Trojan horses, logic bombs and malicious progranms generally are still very mush with us. Virus specifie methods are in the end doomed to failure as a general detection method. Ther come into their own when it is thought that a virus enfection exists and needs to be eradicated.

FLUSHOT+ even states in bold letters, that the best defence against malicious programs is not FLUSHOT+, but "FULL AND ADEQUATE BACKUPS". Thieir capitals, but I could not agree more. No matter what proection you use, it will no doubt be vircumvented one day. Backups are the only real answer to this problem.

When I first tried FLUSHOT+, I encountered what seemed at the time a major problem: FLUSHOT+ would not execute properly from my hard disk. My computer has three floppy disks installed as drives A:, B:, and C:. Therefore my hard disk is drive D:. FLUSHOT+ insisted on executing from drive C:.

After perusing the manual for some time, I admitted defeat and phoned Jim Bates - the UK distributor of FLUSHOT+. He soon solved the probelm. A utility called FLUPPOKE is provided with FLUSHOT+ which lets you change the location of the data file used by FLUSHIOT+. Changing the location of this file was all that was required. The location from which FLUSHOT+ executes is irrelevant. It would make life far easier all round if this was explained in the manual. I hadn't put two and two together and twigged why FLUSHOT+ always insisted in looking at drive C:. A decently explained installation section, with copious examples, would have helped matters.

FLUPOKE is not the easiest of beasts to operate. God knows why this utility required the full pathname for the FLUSHOT+ executable file as a command line argument, and then asked me questions to obtain the location of the FLUSHOT+ data file. Either command line arguments or user questions can be used by computer software, but surely not a muxture of both!

Installation proceeded. Even though I told FLUSHOT+ where its data file was located, I inadvertently forgot to change the contents of this file from the default values, which still pointed FLUSHOT+ towards drive C: for the files requiring cchecksum verification. FLUSHOT+ then found that it could not find COPMMAND.COM in drive

C:, and MS-DOS requested that I choose from the usual "Abort, Retry, or Fail" options. I chose Abort. The computer promptly hung, and even refused to accept the normal Ctrl-Alt-Del reboot keystroke combination. I had to power down and reboot to recommence work. I found from experimenting that the Fail option permits FLUSHOT+ to continue, but this is not particularly helpful when Abort is the most obvious choice.

If FLUSHOT+ was an expensive program, I would probably be suggestng that an idiot-proof installation package should be included. At the cirrent price, you just have to put with the rough edges. Once installed as a Terminate and Stay Resident (TSR) program, FLUSHOT+ occupies just over 16 Kbytes of memory.

Interestingly, the utility that I routinely use to examine the TSR programs currently residing in memory (MAPMEM.COM, a commonly used public domain utility), showed that the section of memory used by FLUSHOT+ belonged to a program called COMMAND, not to FSP.COM, the FLUSHOT+ executable program. The MS-DOS command interpreter is called COMMAND.COM. This is curious and I cannot explain it.

Sidekick is one of the most common TSR utilities used with MS-DOS. No unusual proglems are encountered when Sidekick is resedent in memoty before FLUSHOT+. I loaded Sidekicjk after FLUSHOT+ , in accordance with the manual. FLUSHOT+ correctly triggered when a write to a protected file occurred. However when the user informs FLUSHOT+ that the write should go ahead, the screen characters become underlined throughout, and Sidekick apparently disappears from memory. Very strange.

I'm sure that all of this just illustrates the difficulty of writing TSR programs which do not interact. Both FLUSHOT+ and Sidekick are TSR programs. The safe way to use FLUSHOT+ and Sidekick together seems to be to install FLUSHOT+ last, even though this contradicts the Sidekick manual which states very definitively that Sidekick must be loaded last. Loading FLUSHOT+ last also prevents you from removing Sidekick without rebooting.

I encountered one problem quite frequently. Regardless of whether FLUSHOT+ was triggering on the name of an attempt to delete, read, or wirte to a protected file, FLUSHOT+ always triggered correctly, but the name of the program attenpting the write to file could be erroneous. The name of the previous program used was substituted in place of the name of the current program. The problem disappeared when Sidekick was not present, once again an interaction between TSR programs.

Whenever FLUSHOT+ is operating it puts a '+' symbol in the top right corner of the screen. This can be turned off, and changes to a '-' sign when FLUSHOT+ is resident but disabled. All very good, but many programs also use this location. I have in the past written a large security program which displayed a badge in exactly the same place on the screen. To prevent annoying clashes, it should be possible to specify where the FLUSHOT+ badge is located.

I left FLUSHOT+ operating on my computer for a couple of days, and found that when using a modem to download messages, the computer would not always operate correctly. Aobut 50% of the time the communications program (Odyssey, from Micropack in Aberdeen) 'froze', and the computer had to be powered down to restart things. I've used the same communications software for about six months, at least once a day, with no sign of this problem. Removing FLUSHOT+ cured the problem. Such problems probably show up with communications software as they control the modem using interrupts. I guess that some clash with FLUSHOT+ happened. The problem did not occcur at any consistent location, which also points towards interrupt problems. I did not encounter this problem when using the Eazilink and Procomm communications packages.

Having your computer freeze while communicating with an external computer can cost money. The external computer may think that you are still logged in and continue charging. The only way out of the problem is via a reboot. This always drops the line to the external computer, therefore you cannot logout even if you want to. Some systems do not always respond very promptly when users do not logout in the proper manner.

FLUSHOT+ takes control of many interrupts pertinent to the MS-DOS operating system. Expressed in hex notation, these belong to the system timer (8), Disk I/0 (13), program termination (20), operating system function call (21), absolute disk write (26), terminate: fix in storage (27), operating system reserved: undocumented (28) and floppy disk I/O (40). Any program so closely tied into MS-DOS needs to be very careful about how it interacts with other programs. FLUSHOT+ seems to be somewhat cavalier about such matters, and does not touch upon this problem at all in the mnanual. A serious omission.

All these points are fairly minor, and don't unduly detract from the usefulness of FLUSHOT+.

What effect does FLUSHOT+ have on MS-DOS speed of execution? I tested this by copying 60 short files, each 804 bytes long. When FLUSHOT+ was not active, this took 30.6 seconds. When FLUSHOT+ was active, the copying time increased to 37.8 seconds: a 5% increase. I could not measure any increase in the time taken to delete the same set of 60 files (1.5 seconds). Both of these figures show that FLUSHOT+ does not impose an unduly large overhead on MS-DOS.

One last problem, which is porbably insoluble. The MS-DOS command "DEL A*.*" which deletes all files starting with 'A', triggers FLUSHOT+ even when there are only two files that fulfil this wildcard specification, both of which can be deleted. It should be possible for FLUSHOT+ to look at the disk, find the files that match the specification, and determine for itself that nothing illegal was being done. Instead, it requires the user to provide the answer.

The version of FLUSHOT+ in circulation in the UK comes with a program (called SCANNER) which searches for the patterns of known viruses, such as those published in *Virus Bulletin* every month. It only owrks with parasitic viruses (those that attach themselves to files). Also included with SCANNER are a set of files that contain the patterns of known viruses. The infective part of the viruses have been omitted.

SCANNER worked with all the test patterns provided, and successfully detected real copies of the Cascade, Vienna and Jerusalem viruses: the only three parasitic viruses I tested it against. SCANNER thought that the specimen of the Jerusalem virus also contained the Suriv300 virus, just as predicted by the table of signatures in *Virus Bulletin*. However this is not the fastest of programs. Even on a hard disk, it took 1 minute 55 seconds to check 3.8 Mbytes of executable files when searching for only the Jerusalem virus. This rose to 6 minutes 2 seconds when searching the same disk for 15 viruses (currently the maximum number of viruses that SCANNER can search for). These timings correspond to a search rate of 33 Kbytes per second and 10 Kbytes per second respectively.

At this sort of speed, no-one is going to execute SCANNER very frequently. It's simply too slow. SCANNER seems to search throughout the executable files for the virus signature. However the viruses that it searches for are known to reside only ate certain locations in the file. Perhaps a more intelligent search which took account of this fact would drastically reduce the search time.

FLUSHOT+ comes with a 44 page manual. This does not contain an index and the Table of Contents is of little use for finding things. For instance I could not find any reference to the utility FLUPOKE without searching through the manual work by work. There is also a lack of discussion in the manual about the order in which TST programs should be loaded.

I feel that overall FLUSHOT+ is a program with some loose edges. It has gone through many versions, with steady improvements. for the purchase cost involved, what do you expect but a few loose edges? Apart from the problems described above, I found the product excellent. In the value for money stakes, FLUSHOT+ beats most things I've come across recently.

In conclusion, the main strength of the type of protection offered by FLUSHOT+ is that it does not five a damn whether a detected violation comes from a virus, a Trojan Horse, or a plain old software bug. It stops all of them. This is vitally important.

It is how programs offering protection (as opposed to detection) should operate. The idea propagated by the media that damage to computer data is now coming uniquely from viruses is erroneous.

Technical details

Product: FLUSHOT+

Developer, vendor in the US: Ross M. Greenberg & Software Concepts Design, 594 Third Avenue, New York NY 10016, USA.

Vendor in the UK: Jim Bates, Bates Associates, 64 Welford Road, Wigston Magna, Leicester LE18 1SL, UK, Tel 0533 883490.

Bulletin Boards available for contact: USA (212) 889 6438, UK 0533 880114.

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

Version evaluated: 1.6

Price: Registration cost in the USA is $10 plus $ for postage and packing. In the UK registration can be done through Bates Associates (see above), for the same sums in pounds sterling.

Hardware used: 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 Hard-card, running under MS-DOS v3.30.

EVENTS

The Fifteenth Annual **Computer Security Conference** of the Computer Security Institute takes place in Altlanta, Georgia, USA from 13-16 November. Tel 508 393 2600

S&S Consulting Group is holding a one-day **seminar on the Virus Threat**. It takes place on 16 November 1989 at Rickmansworth, Herts, UK. Details from S&S Enterprises, Tel 0494 791900.

Sophos Ltd continue a series of **Virus Workshops**. The next available workshops are on 21 November 1989 and 25/26 January in Oxford and London respectively. Both technical and general management streams are available. Details from Karen Richardson at Sophos, UK, Tel 0844 292392.

The **Annual Brief on Secure Systems**. This update on computer security developments worldwide takes place on 28-30 November, 1989 at the Hague, The Netherlands. Tel +31 3403 79597.

Corporate Computer Security '90, 13-15 February 1990, Novotel, London, UK. Details from PLF Ltd, UK. Tel 0733 558571.

IFIP/SEC '90. The sixth international conference and exhibition on information security, Espoo, Finland, 23-25 May 1990. For details contact Congrex, Finland, Tel +358 0 175355, or Jugani Saari, Finland, Tel +358 0 177901.

SECURICOM '90. Computer and communications security conference, La Defense, Paris, France. Details from SEDEP, 8 rue de la Michodiere, 75002 Paris France, Tel +33 1 4742 4100.

SICUR '90. Computer security conference exhibition. Madrid, Spain, March 13-16, 1990. Details from IFEMA, Avda de Portugal, s/n 28011 Madrid, Spain. Tel +34 1 470 10 14.

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