October 1992 ISSN 0956-9979

VIRUS BULLETIN

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

Editor: **Edward Wilding** Technical Editor: **Fridrik Skulason** Executive Editor: **Richard Ford**

Editorial Advisors: **Jim Bates**, Bates Associates, UK, **Andrew Busey**, Microcom Inc., USA, **Phil Crewe**, Fingerprint, UK, **David Ferbrache**, Defence Research Agency, UK, **Ray Glath**, RG Software Inc., USA, **Hans Gliss,** Datenschutz Berater, West Germany, **Ross M. Greenberg**, Software Concepts Design, USA, **Dr. Harold Joseph Highland,** Compulit Microcomputer Security Evaluation Laboratory, USA, **Dr. Jan Hruska**, Sophos, UK, **Dr. Keith Jackson**, Walsham Contracts, UK, **Owen Keane**, Barrister, UK, **John Laws,** Defence Research Agency, UK, **David T. Lindsay**, Digital Equipment Corporation, UK, **Yisrael Radai,** Hebrew University of Jerusalem, Israel, **Martin Samociuk**, Network Security Management, UK, **John Sherwood**, Sherwood Associates, UK, **Prof. Eugene Spafford**, Purdue University, USA, **Dr. Peter Tippett**, Certus Corporation, USA, **Dr. Ken Wong**, PA Consulting Group, UK, **Ken van Wyk**, CERT, USA.

CONTENTS

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

EDITORIAL

Window Shopping

On September 15th, *S&S International* unveiled a long-awaited stablemate for its existing anti-virus product range: *Dr Solomon's Anti-Virus Toolkit For Windows.* This coincided with the release of version 6.0 of the highly successful *MS-DOS* version of the product. This new line was launched at the *Business Computing '92* exhibition, where jaundiced hacks had gathered to compare the tinctures in the *S&S* 'hospitality suite' with those of other, larger companies. The good Doctor himself was there to launch what must surely become a monstrous best-seller. As the big moment arrived, an expectant, almost reverent, hush fell upon the room. Dr Solomon entered, brandished a potato crisp briefly at the journalists, and began.

The most striking aspect of the *Windows* version of the software is its exquisite presentation; the *S&S* team has clearly been burning the midnight oil for some months. The use of the *Windows* GUI was clever; the screen was well laid out and clearly much creative and aesthetic thought has gone into the choice of icons. The package is littered with weird and wonderful images, some of which border on the hallucinogenic; one-armed bandits, aerosol cans which vomit green spray (in homage, perhaps, to The Exorcist?) and a piratical skull and cross-bones are but a few of the gems to be found within this veritable treasure trove. As the screen became ever more psychedelic, it was hard not to wonder at the minds which had produced this rapid-fire slideshow of images.

Disinfective capabilities were not demonstrated at the launch, but presumably these have equally psychedelic special effects. After viewing the software, it is only too easy to imagine a panoply of windows filled with gaudy, mesmerising animations showing a menagerie of viral monsters being dismembered by the broadsword wielding *S&S* warlords. The product is crammed with innovative and eye-catching icons, and it was on these novelties that the launch focused.

The *Toolkit for Windows* detects hundreds of viruses, and is capable of cleaning a disk faster than most household liquid detergents. It comes with an impressive pedigree and provides all the buttons and switches that a user could ever want. Only one question remains... is this software really *necessary*?

The implications of a *Windows* based virus scanner are far-reaching. Before executing the scanner, the machine is almost certainly booted from the hard disk. All the relevant device drivers are loaded, and then, at some point subsequent to booting, *Windows* is loaded and executed. Several steps later, the anti-virus software is run. At *every single stage* of this sequence a virus could become resident in the memory of the machine. Once a virus has become memory-resident it can subvert any attempts to search for it, using a variety of techniques.

The need for a virus-free environment was openly admitted by Dr Solomon at the launch: 'For ultimate security you must boot from a clean floppy disk' he told the journos. The next step is to run the trusty DOS version of the Toolkit. Fortuitously, this is supplied free with the *Windows* version!

Entrepreneurs often make their fortunes by developing products of questionable necessity - virtually every city in the country, for instance, has a vendor of giant inflatable bananas, dancing coke cans, plastic bosoms and other such vital commodities. 'Never underestimate public taste' and 'Give 'em what they want' are mottos which guarantee sales. All products (inflatable bananas and plastic bosoms included) are produced because they make *money*. The *Toolkit for Windows* is no exception, and will certainly turn a pretty penny for Alan Solomon. Unfortunately, this product has no sound conceptual basis - from a security viewpoint it is flawed. A single PC may be protected adequately by a *Windows*-based scanner - the risks of such a decision are negligable for a stand-alone machine. However, for protecting a hundred, a thousand, or ten thousand PCs only the best should do. Alas, yes, this implies a return to boring old fundamental principals.

VB's mole at *S&S International* maintains that there has been much agonising within the company over the decision to develop a product which so unashamedly sacrifices security in favour of glitz. It is understood that the *Windows* version of the *Toolkit* was produced simply because of the large size of the perceived market.

While there is no harm in pandering to the masses (indeed, this is a sure-fire route to success) one wonders exactly how far this trend will continue. Will PC users, one day soon, be donning rubber bodysuits to embark on 'virtual reality' anti-viral combat? 'Hands on virus disassembly' could gain a horrible new meaning. The special effects people are standing by. Sigourney Weaver has been auditioned.

The doubts raised here apply equally to any anti-virus package designed to be run under *Windows*. Anti-virus software should be judged on its ability to *detect* viruses and on its inherent security (or lack thereof), and not on its looks. Security can be handsome, but pretty icons, however attractive they may be, are extraneous to requirements. In matters of security, functionality is the key. Any users who seriously wish to protect their computers must not let their hearts rule their heads. Software packages should stand or fall on their real merits: their ability to do the job.

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

CONFERENCE REPORT

The Second International Virus Bulletin Conference

It hardly seems a batting of the proverbial eye-lid since the inaugural *Virus Bulletin* conference, and now the second *VB* event is over! This year's conference was larger than the first, with 207 delegates from twenty countries converging on the beautiful (and wet!) city of Edinburgh. This made *VB '92* the biggest ever 'virus gathering' to date.

The first event of the conference was the speakers' dinner which began, as all good things should, in the bar. This gave the speakers the chance to sample the *Balmoral Hotel's* fine range of whisky, and to meet a spectral apparition who proved a source of speculation throughout the evening. Many voiced their opinions as to who *exactly* this ghostly companion was, but in order to protect the guilty and the innocent, none of their suggestions will be repeated here.

Conference Themes

As last year, there were continuing complaints from the delegates that researchers are too obsessed with collecting and classifying new viruses. Many picture these researchers collecting viruses like stamps and trading them like school-boys in the playground. Given that there are now well over 1500 known viruses, with fewer than a hundred normally seen 'in the wild', this does seem a reasonable criticism. Jim Bates summed it up neatly: 'What are we doing to help the *user*?' - a question which everyone involved in the anti-virus community should continually ask themselves.

Users care about *detection* and *recovery*, not about esoteric debates as to the relative virtues of various strains of the Jerusalem virus. Outside the carefully controlled world of virus research labs the information that users need about a virus includes:

➤ What has it done to my computer?

➤ Has it done any damage?

➤ How do I get *rid* of it?

Speakers Corner. (Clockwise from back left) Joe Norman (*Inmos Ltd*, UK), Jonathon Lettvin (*Lotus Development Corporation*, USA), Dr Jan Hruska (*Sophos*, UK), Dominic Storey (*Novell*, UK), Steve White (*IBM T J Watson Research Centre*, USA), Fridrik Skulason (*University of Iceland*, Iceland), Christoph Fischer (*University of Karlsruhe*, Germany), Roger Riordan (*Cybec Pty Ltd*, Australia), Paul Faulkner (*Barclays Bank plc*, UK), Edward Wilding (*Virus Bulletin*, UK), Jim Bates (*Bates Associates*, UK), Vesselin Bontchev (*Virus Test Centre*, Germany), Dennis Steinauer (*NIST*, USA), David Ferbrache (*Defence Research Agency*, UK), Chris Johnson (*University of Texas*, USA), Mick Wigfield (*Centre-file Ltd*., UK), Barbara Cookson (*Titmus, Sainer & Webb*, UK), Noel Bonczoszek (*Computer Crime Unit*, UK), Rod Parkin (*Midland Bank plc*, UK), Ferenc Leitold (*Hunix Ltd.*, Hungary), Jeff Kephart (*IBM T J Watson Research Centre*, USA).

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

This divergence of emphasis between the parties concerned was already apparent a year ago (see *VB*, December 91 pp. 2 - 5). Reasonable and realistic demands must be dealt with for the good of the industry, which must not forget that it exists to serve the end-user.

The onslaught of new viruses has led many people to develop automatic methods of analysis. This year saw the presentation of several new ideas aimed at accelerating the task of classifying and disassembling new specimens, either by cross-correlation with other viruses, or by a variety of virus analysis languages. Most virus researchers are insomniacs, and are happiest burrowing away into the early hours, their veins awash with caffeine, their eyes scrutinising a vintage copy of DEBUG. These researchers are unworldly, eccentric creatures, and are all individual in their approach; whether automating virus analysis will be universally acclaimed is open to debate.

The long arm of the law is now beginning to feel the collars of the perpetrators of 'high tech' crimes such as virus writing. With the introduction of the *Computer Misuse Act 1990*, computer users within the UK are no longer defenceless against the questionable activities of 'Cracker Jack' and his ilk, though as yet the implications of this new act are not well known. Barbara Cookson, a solicitor from *Titmus Sainer & Webb*, guided the delegates on a useful tour through the complexities of the Act. The SysOps of virus exchange bulletin boards would do well to acquaint themselves with Section 3 of the Act: they are committing an offence which could lead to a five-year jail sentence.

Cookson stressed the need for reliable reporting of virus incidents in order to assist the police with their enquiries. Most people would report a break-in to the police even if nothing were stolen - the same ethical rule should apply to incidents of computer hacking and virus outbreaks.

It is hardly surprising that many people are still unaware of the laws concerning computers and computer crimes, as there has been little publicity given to the *Computer Misuse Act*. In a survey conducted by *Computer Weekly* dozens of respondents did not know of the Act's existence, including two party parliamentary candidates who had worked in the IT industry for most of their lives. Given the serious nature of these issues it is important that the legal position is clear to all - in order for the law to have a deterrent effect upon potential virus writers they must be aware that they can face imprisonment and hefty fines.

VB '92 was not all work, work, work. Here, Mike Lunt of the Home Office receives a round of applause from delegates on his 28th wedding anniversary

Sadly, even though virus exchange bulletin boards are now illegal in the UK, this legislation cannot hope to be effective until there is some international cooperation to prevent the exchange of virus code. Until then, any such board may remain open in areas not covered by this or similar laws.

A Problem Shared...

In an effort to stop the cut-throat competitiveness which is seen throughout the MS-DOS anti-virus community Steve White of *IBM* suggested pooling resources and sharing virus disassemblies. Such a suggestion is enough to cause apoplexy for the chieftains of the warring tribes, as they dance around their respective totem poles. In order to stop the exchange system being dominated by any single group there need to be rules. As White put it: 'You're worried about the rules, right? Well let's make the rules simple: the rules are that there are no rules'.

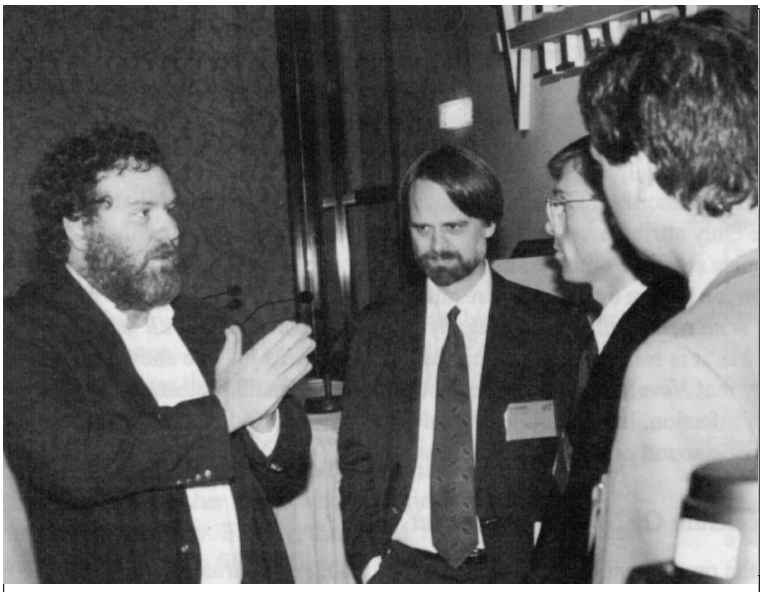
This apolitical approach has been used by the Macintosh community for some time with astonishing success, and White sees no reason why it could not be even more successful for the MS-DOS virus community. Apart from the animosity within the research community itself, the fundamental problem is persuading people to forget their short term financial concerns and see things from a more long-term perspective - sharing code means less research time for all. In order to benefit the community as a whole, *Virus*

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

Bulletin has always published its search strings for viruses and will do so for the foreseeable future. In the long term, cooperation is the only way forward. In the meantime, however, there seems little hope of an end to the internecine warfare being waged in the PC anti-virus community - only time will tell.

...Is A Problem Doubled

One of the most controversial aspects of the conference this year was the publication by *IBM* of statistics and calculations concerning the rate of spread of computer viruses. Until the publication of this paper, the seminal work in this field was by Dr Peter Tippett, who claimed that the prevalence of computer viruses would grow exponentially, until approximately 20% of all computers were infected. On first inspection this seems unrealistic, as it does not take into account any interaction by the user. In the last year we have seen a measurable decrease in the susceptibility of many computers to infection, due to increased awareness on the part of the user, widespread dissemination of anti-virus software, and centralised reporting and response. *IBM*'s statistics show that the growth in the number of incidents is linear rather than exponential, and that this increase is approximately 0.5 incidents per 1000 PCs per year. The wildly inaccurate estimates of the prevalence of the Michelangelo virus have underlined the need for caution in extrapolating infection statistics from a complex data sample. In 1991 *Dataquest* conducted a survey of computer virus prevalence, by putting a number of questions to those responsible for computer virus protection in large organisations. It was the results from that survey which seemed to indicate that the computer virus problem was very large indeed. Kephart claims that the original data samples used by *Dataquest* did not represent the true picture due to an unclear wording on their survey forms. When considering statistics of this kind it is important to remember the prejudices and vested interests that may be concealed within the results. Both *Dataquest* and Dr Tippett are sponsored by firms who produce anti-virus software and *IBM*, which manufactures PCs, may have an interest in belittling the seriousness of the virus problem.



Can man speak without moving his arms? Fred Cohen, hands firmly glued together, attempts to communicate to Steve White and Jeff Kephart the error of their ways.

In the wake of the Michelangelo 'frenzy', a scientific approach is urgently needed. The question of how these figures should be estimated led to a heated debate after the talk between Fred Cohen and Kephart and White of *IBM*, which spilled over into the lunch break - it seems that the formulation of such an epidemiology will prove a time-consuming and highly contentious process (see photo!).

Another welcome set of statistics came from Noel Bonczoszek who presented prevalence data collected by Scotland Yard's *Computer Crime Unit*. This is the first time that the *CCU* has chosen to present this information publicly. The data shows that while there have not been a large number of reports to the *CCU*, the sites which *have* been hit have been hit hard - for example, many of the machines reported as being infected with the Spanish Telecom virus (more than 750) were all involved in the same incident.

Once within an organisation, a virus can often spread like wildfire, contained only by the barriers which go to make up departments or companies. The situation is rather like the threat of being hit by a car; it is unlikely to happen to you, but unpleasant if it does. It is therefore vital that adequate precautions are taken - this means a frequently updated, well written scanner, and preferably some kind of integrity checker. The statistics show that nearly all incidents are caused by a handful of viruses. Therefore the 'scanner A detects 200 more viruses than scanner B' argument should be summarily dismissed when considering the relative merits of anti-virus software.

Home grown can be best

It is often educational to see how a corporate anti-virus policy is put together. The conference was lucky to have two extremely good talks on this subject; one by Paul Faulkner of *Barclays Bank PLC*, and one by Mick Wigfield of *Centre-file Ltd*, a computer

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

services company. At long last, it seems, large companies are becoming less reluctant to discuss the issue of virus protection publicly.

Barclays has taken a novel approach by developing its own proprietary virus scanner and disk error detection system, known as *DEDS+*. When *Barclays* first became aware of the computer virus problem it decided that no contemporary software package provided either the reliability or the support that they required, and that nobody was prepared to offer a global licence which was affordable. It was a relatively simple step to decide to develop its own diagnostic software. As the number of viruses spirals, however, the difficulty in maintaining *DEDS+* will increase. It is an open question whether *Barclays* would take the same decision today. This move towards scanning for viruses at the same time as checking the disk's integrity seems to be a logical one, as both tackle different aspects of the same problem: data loss.

Centre-file Ltd first became painfully aware of the virus threat when it was hit hard by the Cascade virus. However, rather than using a purely 'home-brewed' solution, a combination of commercial products and 'in-house' software is deployed in order to provide the desired level of cover. Two commercial scanners are used within the company - one to scan every new disk which enters a PC, the other by the engineers and technicians when they are called upon to investigate suspected virus situations. This is analogous to a professional bodyguard and his selection of weapons - a man-stopping revolver supported by a rapid fire automatic. In addition to scanning disks, a fast home-grown checksummer is used to look for any alterations to files on the disk. This is used once a day, and once a week a more thorough check is done. This regime has led to extremely effective results - since these anti-virus defences were set up in 1989 *Centre-file* has stopped all viruses 'at the door'.

Some day all viruses will be built this way!
Vesselin Bontchev outlines his chilling vision of the future.

Execute Only?

At the conference this year, much of the discussion centred around the security of *Novell* networks, and as is common in this industry, there was further lively debate as to the propagation of computer viruses on networked systems. The first speaker of the conference, Fred Cohen, discussed how the access rights of a file inhibited or enabled virus propagation under *Novell NetWare*. This had been done experimentally, by setting up a server running *NetWare* and allowing various viruses to attempt to infect it under controlled conditions. Cohen states that the complexity of the *Novell* file Rights system mean that it is possible for a seemingly insignificant change to lead to counter-intuitive results. He has identified by trial and error the Rights and Attributes necessary to secure *NetWare*. Supervisor, Modify, Access Control, and Create must be disabled. Additionally, Write must be disabled *or* Read Only must be enabled! By far the most surprising result Cohen presented was that setting the attributes of a file to Execute Only does not stop the spread of companion viruses, even though the supervisor himself cannot scan the contents of files labelled as Execute Only.

The following morning Dominic Storey from *Novell UK* claimed that the Execute Only attribute *does* provide protection against viruses and that all executables should be marked as Execute Only and Read Only. The contradiction between Cohen and Storey's results means that, quite simply, one of them is wrong. With many millions of Megabytes of data stored on *Novell* servers worldwide, it is somewhat alarming that Cohen claims to have shown experimentally that *Novell's* solution does not provide adequate protection from the threat of infection. It is incumbent upon *Novell* to resolve this conflict quickly and provide sound protection guidelines.

To Checksum Or Not To Checksum?

One of the preoccupations of companies producing anti-virus software is the growing number of polymorphic viruses which are relatively difficult to detect using virus-specific software. Traditional wisdom dictates that some form of integrity checking method be used. However, since many viruses now aim to avoid detection by memory-resident monitors and scanners, it is inevitable that

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

viruses specifically designed to avoid detection by integrity checkers will also be seen. Vesselin Bontchev's paper dealt with the issue of subversion; more specifically, he outlined techniques by which integrity checkers can be undermined. He concluded that there are many ways in which a virus can avoid detection by a badly-written integrity checker. The important thing to note is that it is impossible, if using a well-written integrity checker, for a file to become infected without the change being registered. The vital things to remember are:

- The integrity checking software and its checksums should always be stored on a floppy disk.
- The PC should always be booted from a write-protected system disk.

In an interesting *Gedanke* Bontchev proposed a model for a virus and considered how it would replicate, slipping past the watchful eye of an integrity checking program. Against a 'slow' infector such as this virus, an integrity checking program does not provide any protection. As the operating system *itself* modifies or creates a file, a slow infector strikes, infecting the target file. While an integrity checking program will alert the user that this file has changed this will be of no surprise, as the host file is either new to the disk or has been altered for some perfectly legitimate purpose. While Bontchev is correct in his assertion that a 'perfect' virus of this type would be extremely difficult to detect, its description bears little resemblance to the bug-ridden scraps of code which make up the vast majority of viruses encountered to date. The apocalypse is nigh, says Bontchev, but the rest of the world waits to be convinced.

False Positives

The greatest mirth was caused by accident. One of the acts booked to entertain the delegates during the Gala Dinner was a troupe of jugglers; flaming torches comprised its grand finale. Unfortunately, the hotel management had neglected to deactivate the smoke detectors in the ballroom...

Within minutes, the hotel foyer was filled with partially clad guests, rudely awakened from their slumber by the clamour of the fire alarms. This is a perfect example of a false positive. [Among their number was one Nigel Kennedy - he of the violin and 'right on' accent. What a shame! Ed.].

Acknowledgements, as ever, to the organisational acumen of Petra Duffield and her team, who kept the conference running so smoothly. Finally, thanks are due to the delegates who took the time to fill in the assessment forms at the conference - their comments have been noted. The venue for the *Third International Virus Bulletin Conference* in 1993 has yet to be announced. The programme will contain some radical departures - watch this space.

NEWS

Magazine Mayhem - That *PCW* Review!

The October edition of the UK magazine *Personal Computer World* carried a review of anti-virus software by computer journalist Ken Mann. The results of the review caused momentary astonishment to many seasoned observers, as it called into doubt the effectiveness of some of the best known packages in the industry!

Fifteen different packages were run on supposedly infected files in an attempt to ascertain their detection efficiency. The results showed that four of the products (*Norton Anti-Virus, Dr Solomon's Anti-virus Toolkit, IDS Virus-Pro* and *Certus NOVI*) did not detect *any* of the test 'viruses' at all. *PCW* is (or was!) a well-respected publication in the UK and these 'revelations' have sparked a minor controversy amongst the virologists and their customers.

The virus test set consisted of four viruses (Friday 13th, Alabama, Kennedy and MIX 1A). The selection of viruses is bizarre - the test set is far too small to conduct an accuracy test and it is unrepresentative. While it is not strictly necessary to test a scanner against many hundreds of different viruses, any sensible review should try to select samples which are either particularly hard to detect (such as those which are self-modifying) or particularly prevalent in the real world. The *PCW* review did neither and this was its most obvious error.

The reason that four of the packages did not identify any of the viruses is more subtle. The viruses were described by the reviewer as 'dead', that is, they were not capable of replicating. Exactly how they were disabled is not known, but the wording of the article and the results of the test indicate that the initial JMP or CALL instruction of the virus had been modified so that it no longer executed the remainder of itself. Due to the ever-increasing number of viruses, anti-virus software producers are continually looking for ways to speed up their scanners. One way to do this is to examine the first instruction of a file, and then selectively search areas pointed to by the initial jump for different viruses. This means that if the start of a program has been modified (and the virus completely disabled) a scanner which searches for viruses in this manner will obviously fail to detect *any* viral remnants. Since the virus cannot execute, the correct result a scanner should return is that all the files were clean. Clearly, the *PCW* test was fundamentally flawed.

The danger of product reviews in the popular press is that there is a dearth of specialist knowledge to spot mistakes such as these in the review procedure.

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

It is surprising that such a woeful and ill-conceived test passed the watchful eye of the *PCW* editorial staff. While they could forgivably have been unaware of this innovation in scanning techniques, a test in which products score all or nothing should arouse suspicion in any inquisitive mind ❑

Ghosts In The Machine: *ST Format's* Accident

The thought of releasing software infected with a virus is, for a software distributor, the stuff of which nightmares are made. Even though the vast majority of software houses are intensely aware of the problem, it is easy to let a careless mistake bring disaster upon production. Exactly such a disaster befell the producers of the monthly magazine *ST Format*, which distributed a cover disk infected by the 'Ghost' virus with the October edition of the magazine.

ST Format is aimed at users of the *Atari ST* computer. The first the magazine knew of the infection was when subscribers began to telephone in, complaining of unusual behaviour of their machines. It was quickly realised that the disks were infected, and *ST Format* rapidly began a programme of damage limitation.

Fortunately, the October edition which contained the infected disk had only been posted to subscribers and was yet to be displayed on retail shelves. The edition was immediately recalled. The Ghost virus is well known by users of the *ST*, as it is one of the most common viruses affecting the Atari computer. Fortunately, the virus does not damage data; its only action is to invert the mouse pointer.

ST Format sent all its subscribers an explanatory letter warning them about the disk. This quick action is laudable.

The question remains how the virus infected the distributed disks in the first place. Andy Hutchinson, editor of *ST Format*, explained that the master disk is swept for viruses before being sent out for duplication. When the disks are duplicated, six disks of the pre-production run are sent back to the magazine for checks. It was at this stage that the magazine made the mistake. The master disk was produced late, and therefore the pre-production disks were not scanned. Hutchinson makes no attempt to evade the blame; when questioned about the incident he says 'Ultimately, it was our fault'. He is determined not to let this incident be repeated, and says of the future 'We'll be a hell of a lot more careful - it won't happen again'. The disks (now promised to be virus-free) are being re-manufactured, and the magazine will be available about a week late.

To *ST Format's* credit, they have acted promptly throughout this incident. Hutchinson seems to believe that the best approach to take is to make the information public, and had no objections to being quoted by *VB*. This is the correct way to handle such a situation but it does not excuse the magazine for its carelessness in not checking the disks that were actually sent out. It is easy to be wise after the event, but there is a lesson here to be learned ❑

Beware Old Viruses

One of the latest viruses to be discovered by members of the anti-virus community is the Como virus, which contains the following text:

```
 I'm a non-destructive virus developed to
study the worldwide diffusion rate. I was
released in September 1990 by a software group
resident near Como lake (north Italy).

 Don't worry about your data on disk. My activity
is limited only to auto-transferring into other
program files. Perhaps you've got many files
infected. It's your task to find and delete them
```

If the claim that the virus was written in September 1990 is indeed true, it means it took the virus two years to spread from where it was released, until it was detected and given to a virus researcher. The text could be intended to deceive any authority investigating the origin of the virus, but assuming it is correct this might indicate that a large number of 'old' viruses are in very limited circulation - just waiting to be discovered. Any new virus which is uploaded to a virus exchange BBS becomes almost instantly available to virus researchers, but a virus that is just released on a limited scale may remain undiscovered for a long time ❑

New Viruses Uploaded To UK Bulletin Boards

Two viruses which seem to have originated from the UK have been found within ZIP-type archive files uploaded to Bulletin Boards. Both viruses appear to have been written by the same group which calls itself *ARCV* and whose members' pseudonyms are drawn from cult science fiction.

Neither virus appears to carry any destructive trigger, and the only action of both viruses is to display a text message on certain dates. The text message one of the viruses displays contains the lines 'Made in England' and 'Happy new year from the ARCV'. The larger of the two viruses uses stealth techniques to mask the increased size of infected files.

Both these viruses were discovered as *Virus Bulletin* was going to press. A full report, together with detection patterns, will be published in the November edition. In the meantime, Scotland Yard's *Computer Crime Unit* (071 230 1177) would like to hear from anyone who has information about these viruses ❑

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

FEATURE

Ephraim D. Brand

Viruses and Anti-Viruses in Israel

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 BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

IBM PC VIRUSES (UPDATE)

Updates and amendments to the *Virus Bulletin Table of Known IBM PC Viruses* as of 23rd September 1992. 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

_2623 (temporary name) - EN: Fairly big, but not particularly interesting virus. Awaiting analysis. One 2617 byte variant is known, and can be detected with the same pattern.

```
_2623           33F6 BB0C 00B9 0500 8A07 0414 8842 F643 46E2 F5C6 42F6 00C7
```

Alexander - CER: This virus was first reported in Canada, but is probably of European origin. It contains an encrypted text string, which ends in 'Alexander - Constanta, Romania.'. Alexander is detected with the Dark Avenger pattern, but is quite different. It is not yet clear if the viruses are related at all. This virus is 1951 bytes long.

Backfont-821 - ER: Detected with the Backfont (905) pattern. Awaiting analysis.

Bebe-486 - CN: This seems to be an older, shorter variant of the 1004 byte Bebe virus. Detected with the Bebe pattern.

Cls - CER: An 853 byte Russian virus, which may occasionally clear the screen on an infected machine.

```
Cls             B4FF CD21 80FC F075 03E9 8200 B821 35CD 210E 1F2E 8DB6 1F01
```

Como - EN: This encrypted, 2019 byte virus contains a long text message. It appears to be fairly harmless.

```
Como            D08B DC8C CA8E D2BC 8E00 81C4 8000 5053 1E06 E81F 00E8 0307
```

Creeper-425 - CR: Smaller than the Creeper-475 virus reported before, but detected with the same pattern.

Dark Avenger-Outland - CER: This 2136 byte variant seems to be based on the 1800 byte variant. The text messages have been changed ('Eddie Lives' is now 'Billy the Cat Lives!'), and other alterations made in order to bypass published signatures.

```
Outland         5006 561E 8BFE 33C0 508E D88B C1C4 064C 002E 8984 4408 2E8C
```

Dark Avenger-1947 - CER: This Russian variant is detected with the standard Dark Avenger pattern. The original 'Eddie lives...' message has been replaced with 'If you are a thieve man , virus lives...somewhere always!You must become good man!'

Diamond-Rock Steady-B - CER: Closely related to the Rock Steady variant reported in May, and detected with the same pattern.

Filedate 11-537 - EN: Similar to the older 570 byte variant, and probably of Russian origin. Encrypted. Awaiting analysis.

```
Filedate11-537  501E 060E 1F1E 07BB 1500 2E80 37?? 4381 FB19 027C F5
```

Finnish-257 - CR: This is a shorter variant of a previously known 709 byte virus, also from Finland and probably written by the same author. It is not entirely clear which version is the original. This one does not seem to do anything but replicate.

```
Finnish         F3A5 0633 C08E C026 A184 0026 8B0E 8600 0726 A39A
```

Ier-560, Ier-512 - CR: Two Russian viruses, which are probably by the same author as the Ieronim virus, but are quite different structurally - they place the virus code at the beginning of infected files, whereas the Ieronim virus appends itself to files.

```
Ier-560         80FC 4B75 5306 1653 561E 5250 518B D8B9 3E00 8BF2 8A04 22C0
Ier-512         80FC 4B75 5506 1653 561E 5250 518B D8B9 3E00 8BF2 8A04 22C0
```

Ieronim - CR: A remarkable feature of this 570 byte virus is that it may occasionally display a message in Latin.

```
Ieronim         5B58 0EB8 0001 50CB 80FC 4B75 601E 0616 5356 1E52 5051 8BD8
```

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

Jerusalem-Count - CER: A modified 1813 byte variant which seems to have been created by re-assembling the original code.

```
Jer-Count           2638 05E0 F98B D783 C203 B800 4B06 1F0E 07BB 3500 9C2E FF1E
```

Jerusalem-Zipeater - CER: This 1984 byte variant is awaiting analysis, but the name indicates it might be targeted against .ZIP files.

```
Jer-Zipeater        2638 05E0 F98B D783 C203 B800 4B06 1F0E 07BB 3500 E8CE 041E
```

Junior - CR: A small Bulgarian virus.

```
Junior              813C 4D5A 743B 803C C474 3631 C98B D1B8 0242 CD21 462D 3800
```

KLF - CR: A 356 byte Russian virus which does not seem to do much of interest other than replicating.

```
KLF                 B802 3DCD FD72 AE8B D80E 1FB8 0057 CDFD 72A6 890E 6C03 8916
```

Leprosy-Wake - EN: Encrypted, overwriting virus - 625 bytes long.

```
Leprosy-Wake        BB3F 0190 8A27 9032 2608 0190 8827 4381 FBB0 037E EFC3
```

Leprosy-FVHS - EN: Primitive overwriting virus, 2218 bytes long. Detected with the Leprosy-Silver Dollar pattern.

Little Girl - CER: 1008 bytes long. Awaiting analysis.

```
Little Girl         002E 8B16 0A00 2E8B 360C 002E 8B3E 0E00 2E8B 2E10 00FB C33D
```

Magnitogorsk-3000 - CER: A 3000 byte encrypted Russian stealth virus, which places its code at the beginning of infected files, including infected EXE files.

```
Magnito-3000        50A1 2201 3D00 0074 0FBE 3D01 B97B 0B00 04F6 2E04 0146 E2F7
```

Minsk Ghost - CER: New, variable-length Russian virus. Awaiting analysis.

```
Minsk Ghost         B807 C831 DBCD 2183 FBFF 7503 E91E 011E 5B4B FA8E DBA1 0300
```

Nazgul - CN: The most interesting feature of this 266 byte virus is its ability to evade or disable several virus monitoring programs.

```
Nazgul              BE4D 44CD 2F3D 00FE 7503 EB11 90B8 02FE BF55 4EBE 4D44 CD2F
```

Otto-415 - CN: Probably an older version of the Otto-640 virus, reported as Otto6 last month.

```
Otto-415            E800 005E 5681 EE08 0158 2D00 01A2 FF00 56B9 7B01 81C6 2901
```

Pipi - CER: This virus seems to be derived from the Jerusalem virus, but the modifications are quite extensive. The size is 1552 bytes, but the effects have not been fully determined.

```
Pipi                80FC E075 02B4 EE3D 004B 7437 80FC ED75 0AF3 A458 5858 B800
```

Press - EN: A 1024 byte Russian virus. Awaiting analysis.

```
Press               B9FF FFBA 00FC CD21 7303 E9D3 00B4 3F5A 5281 C274 02B9 1C00
```

Prob-734 - ER: A 734 byte Russian virus. Awaiting analysis.

```
Prob-734            B003 CF9C 2E80 3E12 0300 7402 9DCF 552E 892E EA02 33ED 80FC
```

Red Diavolyata-662, MLTI-662 - CR: A Russian virus, derived from the 830 byte Red Dyavolyata (MLTI) virus.

```
Red Diav-662        5B73 05B8 0001 50C3 83FC E072 F633 C08E C026 C516 8400 2E89
```

Ryazan - ER: An encrypted 512 byte Russian virus.

```
Ryazan              BE?? 00B9 EC01 1E8C C88E D880 34?? 46E2 FAE8 0000
```

Seacat - CN: This 160 byte Russian virus noes nothing but replicate.

```
SeaCat              813C 4D5A 7424 5133 C9B8 0242 CCFE C42E A306 0159 B440 CC51
```

Signs - CR: The name of this virus is derived from a string it contains: 'Signs Of Life'. The virus is of Russian origin, 720 bytes long and has not been analysed yet.

```
Signs               061E 5756 559C 80FC 4B75 E48B F2FC AC22 C074 02EB F981 7CFC
```

Sistor-2630 - CER: Detected with the Sistor-2380 pattern.

Suicidal - CN: A simple, 305 byte virus, containing the text 'Suicidal! -/\-=>[Stingray/VIPER] <1992>'. No obvious effects.

```
Suicidal            C684 D100 E98B 94F4 0083 EA03 8994 D200 C684 D400 10B4 40B9
```

SVC 3.1-CHR - CER: Almost identical to the SVC 3.1 virus, and detected with the same pattern.

SVC 6.0-4677 - CER: Closely related to the other SVC 6.0 viruses, but slightly longer. Detected with the SVC 6.0 pattern

Timemark - ER: Two viruses, 1062 and 1083 bytes long, that have not yet been analysed.

```
Timemark1           B8FF 4BCD 2172 03EB 6F90 0706 8CC3 4B8E DB8B 1E03 0083 EB43
Timemark2           B8FF 4BCD 2172 03EB 6F90 0706 8CC3 4B8E DB8B 1E03 0083 EB44
```

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

Tumen-1242 - CR: This variant, which calls itself v1.3 is somewhat longer than the other known members of the Tumen family, but detected with the same pattern.

UFA-1201 - CN: A 1201 byte Russian virus that infects two COM files when an infected program is run. Awaiting analysis.

```
UFA-1201            8D7E 3FB0 90FC AAB0 E8AA 8B46 172D 0400 AB8D 463F 8946 19C7
```

Ungame - ER: This virus only infected EXE files in testing, but it contains code which seems to indicate it is designed to infect COM files as well. The virus is of Russian origin and is 766 bytes long. Awaiting analysis.

```
Ungame              B8AA AACD 213D BBBB 7465 1E8C D82D 0100 8ED8 BB03 008B 072D
```

Vienna-W13-458 - CN: A member of the W13 group, which marks infected files by setting the month field to 13. The virus is 458 bytes long and is detected with the W13 pattern. The virus originated in Eastern Europe.

Vienna-Twer - CN: A typical Vienna variant - 1000 bytes long.

```
Vienna-Twer         ACB9 0080 F2AE B904 00AC AE75 E3E2 FA83 FF05 7407 2680 7DFA
```

Walker - CER: A 3846 byte virus, which contains a text message claiming it is written in Turkey. It is reported to display a figure walking across the screen.

```
Walker              83C7 02E2 E85F 5E81 C7A0 003E 0376 0C59 E2D0 5D07 1F5F 5E5A
```

XPEH-5856 - CER: A new member of the XPEH group of large, Yankee-related viruses. Awaiting analysis.

```
XPEH-5856           2E8B 0433 C22E 8904 83C6 02E2 F3C3 BEC2 0903 F3B9 4F00 2E8B
```

Yankee-1256 - CER: This variant resembles the 1049 byte variant, which used to be called USSR-1049, but has now been re-classified as a member of the Yankee family. Not fully analysed, but detected with the 1049 pattern.

Youth-Silence - CN: A 555 byte, encrypted virus, related to the Youth and Futhark viruses reported last month. The most unusual feature of this virus is that it partially encrypts the original program, which complicates disinfection slightly. The virus contains the text string 'Silence of the Lambs!', but does not seem to have any particular effects.

```
Silence             EB02 ??59 B9EC 01BE 1401 B4?? 2824 4680 C4?? E2F8
```

VIRUS ANALYSIS 1

Jim Bates

Chad - A Test Case Of Mobile Graffiti

This virus has been named Chad after a cartoon character known in England during the Second World War. The code is about as primitive as it is possible to get and still be a virus and yet has some features that make it worthy of more attention from the law enforcement authorities.

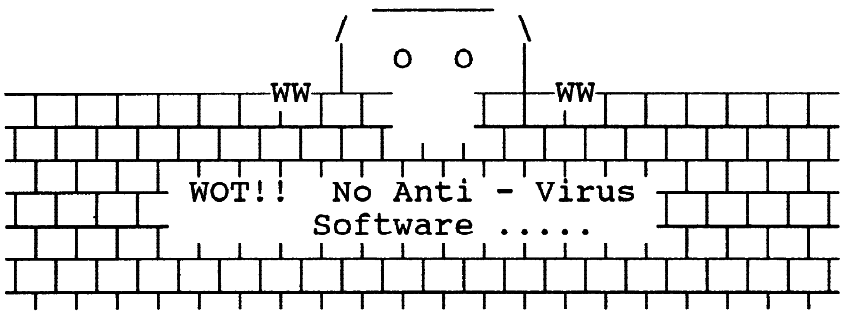
Operation

This is a non-encrypting, non-resident virus that simply appends its code to COM files found within the current directory. Disassembly is therefore not difficult, as the various routines are easily identified and analysed. The virus inserts a CALL instruction (together with an appropriate offset value) at the start of an infected file and this transfers processing into the virus code proper. The code begins with another CALL to the next instruction, where the return location is popped from the stack. This is used thereafter as an index pointer to enable the virus to locate its various data values.

One of these values is a counter which is incremented each time an infected program is run. Since this counter is maintained within the virus code and *not* re-initialised at each infection, over a period of time a number of infected files will contain varying values within this counter. Since the counter is used to decide when the trigger message should be displayed, it is difficult to predict the exact occurrence of the trigger (see Trigger section below). Once the counter has been incremented and checked, the virus repairs the first three bytes of the host program file and then issues a FIND FIRST function request to the system, looking for files with a COM extension. When a matching file is found, the last three bits of the seconds field of the date/time stamp are checked and if found to be zero, the file is assumed to be already infected. In this case, processing loops and continues searching for any other suitable matching files.

Once an uninfected file is found, an attempt is made to open it for READ/WRITE access. If the file has been protected by having the READ ONLY attribute set, the OPEN request will fail and processing is passed back into the search loop. If the file is successfully opened, the first three bytes of the file are read into a buffer area within the virus code and then replaced with the CALL instruction mentioned above. The next stage is to append the virus code to the end of the target file and then the file date/time stamp is cleared to zero (both date *and* time) before the processing is returned to the host file.

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.



Viruses have been compared to mobile grafitti many times in the past, but this is the closest yet. Presumably the same noble motives inspire the writers of both.

unauthorised modification of the contents of any computer; and at the time when he does the act he has the requisite intent and the requisite knowledge.' (Computer Misuse Act 1990, Section 3,1 paragraphs a and b).

The code is poorly written and causes irreparable damage to some program files. If my surmise about it being a demonstration virus is true, there may be many people who have seen it in operation (possibly at training seminars or sales presentations). If so, they should contact the *Computer Crime Unit* at New Scotland Yard.

Trigger

The trigger routine is executed if the counter is an exact multiple of 10. Thus the trigger display should be seen every tenth time an infected file is executed. The display is interesting, quite distinctive and attempts a pseudo-graphic representation of the Chad character beloved of newspaper cartoonists in England during and immediately after the Second World War.

These cartoons featured a crude representation of a humpty-dumpty character peering over a brick wall and always contained a caption beginning 'Wot no ...'. Wartime shortages and rationing, together with barbed observations about political and military activity were all considered suitable for Chad's comment. The point here is that few people outside England or under the age of forty have ever heard of this character and so the display provides some information for investigators interested in identifying the author. In the virus, the caption reads 'Wot!! No Anti-Virus Software .....'. There is also an additional line of text which should be displayed, but is not because of an incorrect variable value in the display routine. This line should be shown above the picture and contains the text 'CHAD against damaging viruses ... Save Our Software. 1992.'

When the trigger routine is invoked and the picture is displayed, the machine hangs and must be rebooted.

Conclusion

This virus may have been written for demonstration or test purposes. In the UK this raises the hoary question of whether or not it is criminal to produce such code. The criterion is whether the code contravenes the provisions of the *Computer Misuse Act* 1990. This states that - 'A person is guilty of an offence if he does any act which causes an

Chad

Type: Non-Resident, Parasitic, Appending.

Infection: COM files of any length (including COMMAND.COM).

Recognition:

File Last three bits of seconds field set to zero.

Hex Pattern

```
8944 0AB4 40B9 EF02 8B14 CD21
B800 4233 C933 D2CD 21B4 40B9
```

System is No recognition in memory as this virus non-resident.

Intercepts: None - this virus is non-resident.

Trigger: Displays crude picture of Chad character with caption - "Wot!! No anti-virus Software .....'.

Removal: Specific disinfection is possible except on files which were originally greater than 64784 bytes, or those which require unhindered access to their original time/date stamp. Otherwise, under clean system conditions, identify and replace infected files.

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

VIRUS ANALYSIS 2

Jim Bates

Groove - Revenge Upon Integrity Checkers?

The Groove virus is yet another specimen which uses the Mutation Engine in a vain attempt to avoid detection. It is a memory-resident COM and EXE file infector which infects programs upon execution. Because of the programming style of the virus writer, and the text displayed when the virus executes its trigger routine, it seems likely that this virus is Bulgarian in its origin. The most interesting aspect of this virus is that it attempts to upset a number of well-known integrity checking programs.

Mutation Engine Encryption

It should first be made clear that just because a virus uses encryption, it is not necessarily more difficult to disassemble. Virus code must be executable, therefore encrypted code must be decrypted before use. Disassembly simply begins a stage later, after the primary decryption routine has been executed.

In this instance, the total infective length of the virus is around 3510 bytes, of which 2202 bytes is the Mutation Engine and its associated random number generator. Since several vendors of anti-virus software have now developed algorithms to identify such code, the 168% overhead this virus carries in its unsuccessful attempt to remain anonymous is totally pointless.

Moving In

When first executed, this virus begins by issuing an 'Are you there?' call to the system, which consists of placing the value FBA0h in the AX register and making an INT 21h request. If the virus is resident, the value 0ABFh is returned in AX. If this is the case, a routine is called which attempts to delete the database files of several well known integrity checking programs before passing control back to the host program.

If the virus is not resident however, the address of the INT 21h service routine is collected by direct access to the interrupt table, and stored within the virus. Next, the top of conventional memory is lowered by 5120 bytes. The virus code is then moved into this memory area and the address of the newly located virus interrupt handling routine is inserted into the interrupt table. This effectively installs the virus as permanently resident and active in memory, and processing now continues with the 'file delete' routine mentioned above.

Integrity Checker Attack

The operation of integrity checking programs varies between vendors but they universally rely upon some form of database which contains details of files to be checked. The Groove virus deletes the relevant databases, the author of the virus presumably acting under the assumption that having had their knickers deleted, the integrity checkers won't feel a draught.

This method of subverting integrity checkers has been seen before. The Peach virus (see *VB* May 92, p.17), which is targeted against the *Central Point Anti-Virus* package, deletes part of the checksum database. Incredible as it seems, this method actually works - when *CPAV* [Certainly for versions 1.00 to 1.20. Ed.] is next run, the software blindly recreates the missing checksum file.

I've heard of fuzzy logic, but this is the first time I've come across true crazy logic.

This gaping hole in security aside, the idea of deleting the checksum files does have a sound basis. Even if the checksumming package does alert the user to the lack of its checksum database, it will not know whether any of the files on the disk have been changed. The Groove virus extends this technique to include several other well known integrity checking programs. Stored within the virus are the following filenames (complete with path):

```
C:\NAV_._NO
C:\NOV|RCVR.CTS
C:\NOV|PERF.DAT
C:\CPAV\CHKL|ST.CPS
C:\TOOLK|T\F|LES.LST
C:\UNTOUCH\UT.UT1
C:\UNTOUCH\UT.UT2
C:\VS.VS
```

Each of these names is accessed by a routine that attempts to delete the file and then increments the drive letter. The whole routine accesses each filename in turn and loops through five invocations, thus trying drives C:, D:, E:, F: and G: . No attempt is made to remove any protective attributes before the deletion - I've heard of fuzzy logic, but this is the first time I've come across true crazy logic. Once this routine finishes, control is returned to the host program.

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

Operation

The installed interrupt handler intercepts just two functions requests - the answer to the 'Are you there?' call, and the familiar LOAD and EXECUTE request (function 4B00h). The EXEC intercept is solely to test the target file's suitability for infection and begins by saving the caller's stack and file pointer values (SS:SP and DS:DX) and then allocating a new stack within the memory block used by the virus. The next stage seeds the random number generator in preparation for later use during encryption and infection.

The target file attributes are then collected, stored and modified to override any READ ONLY settings. Next, the file is opened for READ/WRITE access and the first 28 bytes are read into a buffer area. At this time, the actual length of the file is checked and files longer than 61535 bytes are rejected. Then the header is examined to determine whether it contains the 'MZ' or 'ZM' header, marking it as an EXE type. If the target file is an EXE type, the checksum field of the header (the tenth word) is tested for a value of 0FBAh to see whether the file appears already infected. For other file types, the infection marker (still 0FBAh) appears as the third word in the file.

Once the target file (of either type) has been found suitable for infection, the relevant modifications are made to its header and the virus is encrypted (via the mutation engine) before being appended to the target file. When infection is completed, the file is closed and the attributes reset to their original value before control is finally passed to the original function request routine.

Strangely, no attempt is made to preserve the original date and time stamp of the target file. Thus any infected file will be marked with the date and time of its infection.

Trigger

During the file infection routine, the system clock is checked to see whether the time is between midnight and 00:30 am. If so, the screen is cleared and a message is displayed while processing appends the virus code to the target file. The message (in all its fractured glory) is

```
Dont wory, you are not alone at this hour...
This virus is NOT dedicated to Sara
its dedicated to her Groove (...Thats my name)
This virus is only a test Virus
therefor be ready for my Next Test ....
```

I assume that the Sara referred to is the same Sara Gordon mentioned in the documentation distributed with the mutation engine.

After displaying the message, a final piece of mind-numbingly brilliant coding adds a random number of bytes (between 0 and 63) to the end of the file before passing control back to the host program.

Conclusions

The usual disparaging remarks seem to ring a little thin after so many repeats. There is little that can be said about this virus that has not already been said hundreds of times. A nasty little conception that undermines the very industry that helped to give it birth, this is just another tired addition to the growing list of odious programs produced by malcontents and misfits. If it is indeed Bulgarian in origin, it only supports my contention that any computer technology from that country should be treated with extreme scepticism until they put their house in order.

Groove

Aliases:	Sara's Groove.
Type:	Resident, Parasitic appending.
Infection:	All executed files smaller than 61,535 bytes.
Recognition:	
Files	EXE files : value of 0FBAh in the checksum field of the file header. Other files - value of 0FBAh as the third word in the file. Infective length will be between 3508 and 3700 bytes.
System	'Are you there?' call: FBAOh in AX - call INT 21h returns value of 0ABFh in AX.
Hex Pattern	Simple hex pattern not possible. This virus is encrypted.
Intercepts:	INT 21h for infection and detection of trigger conditions.
Trigger:	Displays message (see text) if system clock is between midnight and 00:30.
Removal:	Specific and generic disinfection is possible. Under clean system conditions, identify and replace infected files.

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

PRODUCT REVIEW 1

Dr Keith Jackson

VirusCure Plus

Through no fault of its own, this product caused a few heart stopping moments before I even started work on the review proper. Following my usual rules, I scanned all of the floppy disks provided with *VirusCure Plus*, using two scanning programs, and to my utmost surprise one of these scanners (*SWEEP* from *Sophos*) informed me that the main executable file (*CURE.EXE*) contained 'Spanish Head', one of the signatures used to detect the Spanish Telecom virus. I followed this up by scanning the floppy disks with four other scanners (*Dr. Solomon's Anti-Virus Toolkit, McAfee's Scan, Vi-Spy*, and *Smartscan* from *Visionsoft*), none of which reported the offending floppy disk(s) as being infected. I can only put this down to a false alarm reported by *SWEEP*. Nonetheless, I made sure that this month's review was carried out on my spare machine, just in case!

VirusCure Plus claims that it 'detects known and unknown viruses', and 'prevents any attempt by a virus (known or unknown) to penetrate and infect'. It detects known virus patterns by scanning, and attempts to detect any changes to files by creating signature files. The package also contains a memory-resident monitoring program which should signal viral activity. If an infection is detected, *VirusCure Plus* is capable of removing the virus from the infected file.

VirusCure Plus was provided on both 3.5 inch (720K) and 5.25 inch (360K) floppy disks, both of which arrived without write-protection enabled. Given the scare that I had regarding these disks being infected (see above), this hardly inspired confidence in the product. I firmly believe that anti-virus products should be distributed on permanently write-protected disks, or, if small volumes dictate that this is not possible, on disks that have been write-protected before the product is distributed.

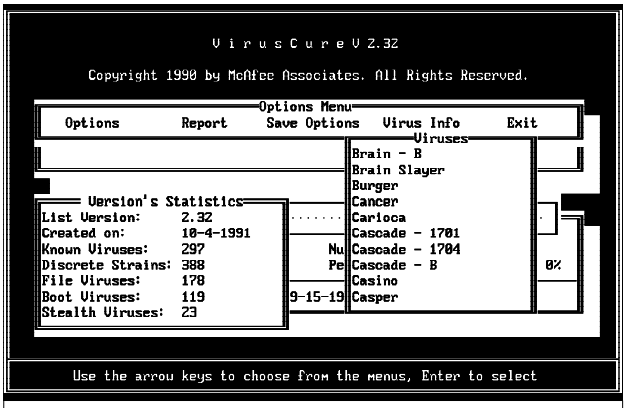
Documentation

The information provided with *VirusCure Plus* is contained in a slim (22 page) A5 'booklet' (manual is too grandiose a word for it), which frankly does little more than describe extremely briefly what *VirusCure Plus* does, and how to install and execute the program. I'm all for simplicity, but this is taking things to extremes. Sections on what to do if a virus is discovered, avoiding re-infection, memory-resident viruses, and general safety measures, are all rudimentary in the extreme - each of them comprises less than a single page. Two pages of this meagre documentation are totally given over to a detailed description of the program's license terms.

Uncertain Pedigree

The documentation states that the file VIRUS.LST contains a list of the viruses known to *VirusCure Plus* (144 in total). However the first page of the VirusCure Plus booklet claims knowledge of 230 viruses, and the sticker on the outside of the box claims that *VirusCure Plus* now 'detects over 893 viruses'. During my testing of *VirusCure Plus*, information on the screen stated that it could search for 297 known viruses, which comprised 388 'discrete strains' (their phrase). I do not know which of these figures is correct. Contradictory information such as this does not help the user. Rather curiously the file VIRUS.LST which is claimed in the documentation to be the definitive list of viruses is only dated 31st January 1991, and the most recent file on the entire floppy disk is dated 5th November 1991, making *VirusCure Plus* hardly the most up to date anti-virus software package [The latest version is v2.41. It is *VB*'s policy to review what we are *sent*. Ed.]. *VirusCure Plus's* origins are rather cloudy as although the software is claimed as the licensed property of *IMSI*, the copyright is assigned to both *IRIS Software* and *McAfee Associates*, both of which are familiar names amongst anti-virus software vendors [The scanning engine appears to be *McAfee's Proscan*, and the memory resident part is licensed from *IRIS*. Ed.].

Installation of *VirusCure Plus* proved to be very simple, though fraught with a few niggling errors (see below). Immediately after installation commences, a screen prompt asks whether you want to look at the README file. Responding 'Yes' proved less than useful as it locked up the computer to the extent that a power-down was required. Replying 'No' to the aforementioned question produces a menu which allows the user to choose between installation, de-installation or reconstructing the boot/partition information. After optionally updating the AUTOEXEC.BAT file, the installation program states that it is ready to write the



How many viruses does the package detect? Every reference to this number is different - hardly a fact to inspire confidence.

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

signature files to floppy disk. However nothing on screen advises the user to change disks at this point, nor does anything in the printed documentation. This point is explained in the README file, though attempting to read this file during installation causes the machine to lock up as described above. Fortunately, I had scanned the README file before attempting installation. Although the user can specify the drive on which *VirusCure Plus* should be installed, the installation program insists on using a subdirectory called VIRUSCUR in the root of the chosen drive. This is poor; good software packages should allow installation in any nominated subdirectory.

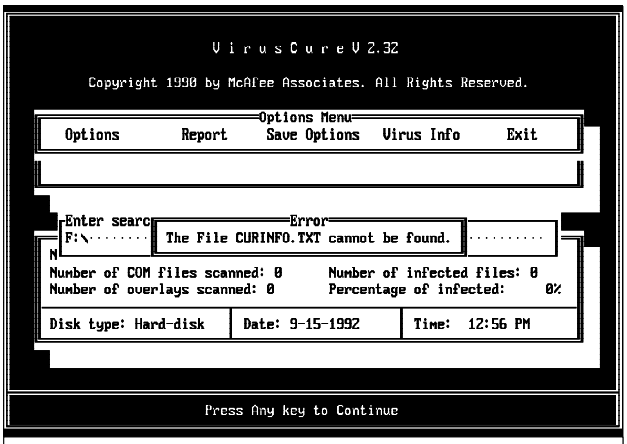
P: ?

Rather curiously, the default drive for de-installation is P:, I've no idea why, as my drives don't actually stretch this far! De-installation successfully removed *VirusCure Plus*, and cleanly replaced the old version of AUTOEXEC.BAT, however it did leave behind a copy of the virus information file (VIRUS.LST) in the root of drive C:. This was most odd as I had installed *VirusCure Plus* on drive F:. All in all, although I found a few odd quirks with the installation process, these seemed to be nothing that more testing would not iron out.

Scanning

Using the *VirusCure Plus* menu system is straightforward. It requires entry of the path to be scanned, with various configuration options made available by pressing the F10 key. The user simply sets up his chosen configuration, specifies the drive to be tested, and optionally names specific file extensions and/or subdirectories. The disk is then scanned after these selections have been made. Operation is possible either under *Windows* or under DOS, both of which executed successfully, albeit with some inconsistencies. For instance, when scanning a floppy disk, if the disk is not fully inserted in the drive, a Retry/Abort message is displayed. Selecting the Retry option causes the computer to lock up. Selecting the Abort option is almost as bad; it aborts the *VirusCure Plus* program and returns to the operating system. These faults only occurred about one time in every three - I've no idea why.

A second problem manifested itself when I tried to produce a report about the previous disk scan. If the scanning process is stopped after a virus has been found, the user is asked whether or not he wishes to scan another drive/ subdirectory. The logical thing is to answer 'No', but this returns straight to the operating system, jettisoning any information to be contained in the report! It is imperative to reply 'Yes', and then use F10 to escape and produce the report. Hardly a logical sequence.



Alas, the installation program has omitted to copy this file across. Errors like this should be spotted at the testing stage.

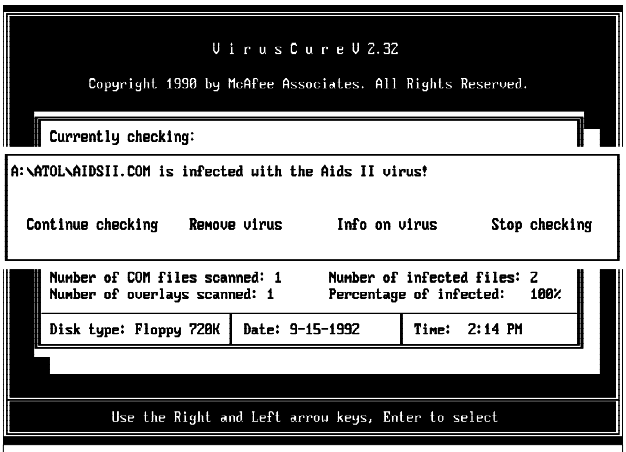
One of the *VirusCure Plus* menu options provides 'Help', i.e. a description of each of the known viruses. This proved to be an excellent feature, with a few paragraphs available on each virus. However it would have been more helpful if the file that provided this information (CURINFO.TXT) had been copied across by the installation program, rather than letting me figure out for myself why *VirusCure Plus* could not find this file whenever the Help feature was activated.

Detection And Removal

VirusCure Plus checked my hard disk (18.2Mbytes contained in 686 files in total, of which 275 were checked), taking 30.8 seconds when executed under DOS. For comparison purposes, when executing under DOS, *SWEEP* from *Sophos* in quick scan mode performed the same scan in 15 seconds, and *Dr Solomon's Anti-Virus Toolkit* took 14 seconds to perform the same task. When *Windows* was used this time rose to 39.5 seconds. *VirusCure Plus* can optionally search inside compressed executable files compressed by *PKLITE* or *LZEXE*, and this increases the scan times to 35.2 and 44.5 seconds respectively. An option is available within the *VirusCure Plus* menu structure to generate a report from each scan, either by writing the report to a file, or by printing it out. This report is available in either 'Short' or 'Detailed' format, but neither of these reports contained information to explain what was actually scanned (beyond stating the disk label), what options were active, or what viruses were found. I'm unsure whether this was a fault or a 'feature'. The documentation does not say anything about it.

Even with a long-standing test set of viruses (see *Technical Details* below), *VirusCure Plus* still failed to detect 29 of the 183 infected samples, a detection rate of only 84%. It failed to detect one version of the Amoeba, Datacrime, Rat, Svir, Turbo488, Lovechild, Violator, Voronezh, 492, and 8 Tunes viruses, two variants of Burger and Vacsina, four

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.



Even though *VirusCure Plus* can optionally remove a virus from an infected file, the usefulness of this is minimised by the program exiting to DOS every time the operation is completed.

of Vienna and Yankee-Doodle, and no less than seven variants of the Tiny virus. This is poor, and is made even worse by the fact that all of the viruses in the test sample predate even the out-of-date *VirusCure Plus* files, which rules out the age of the VirusCure Plus files as an excuse.

Although *VirusCure Plus* can remove viruses from executable files, this option is made less than ideal by exiting the scanner program back to the operating system whenever it is used. This is either a software bug, or a serious design flaw. However, apart from this 'feature', I could find no fault with virus removal, although re-executing the *VirusCure Plus* program for each individual virus made it difficult to test against all the viruses listed in the *Technical Details* section. The documentation states that scanning continues after the virus has been removed. It's wrong.

Memory-resident Protection

The memory-resident part of *VirusCure Plus* is installed directly from the start of the AUTOEXEC.BAT file, and occupies just over 23 Kbytes. However nothing in the documentation actually explains what these memory resident components of *VirusCure Plus* actually do, beyond saying that the two PROTECT programs (why there are two of them I've no idea) will 'scan important sections including BIOS, the COMMAND.COM file, the systems files, hard disk partition table and boot sector'. This short explanation introduces more questions than it answers: Why scan the BIOS which resides in ROM? Why can I alter a byte in the COMMAND.COM file using the *MS-DOS Debug* program without PROTECT complaining? If the memory-resident programs are actually doing something, why can I measure no increase whatsoever in the time taken to copy over a Megabyte of executable files (which could all have been infected) from one subdirectory to another? Exactly what are the 'Systems files' (their plural on both words)? Why does *Dr.Solomon's* virus scanner refuse to operate when the *VirusCure Plus* memory-resident programs are active, saying that it detects the Number of the Beast virus resident in memory? I admit that I eventually gave up; the vague description in the documentation, and the above anomalies, made it impossible to test out the memory-resident portions as sensibly as I would have liked.

Conclusions

Following *VB's* standard policy, we review what we receive, and it must be said that the *VirusCure Plus* files do seem to be somewhat out of date. A scanner program lives or dies by successful detection of viruses, and speed of execution. Although *VirusCure Plus* offers passable execution speed, it's certainly not as fast as some other popular scanners. The detection rate can obviously be improved by keeping the *VirusCure Plus* files more up-to-date. The version I reviewed would never be capable of detecting any virus discovered after November 1991, almost a year ago - and an awful lot of viruses have been discovered since then.

Introducing a memory-resident program which causes another anti-virus product to think that the Number of the Beast virus is resident in memory is unforgivable. It may or may not be a false alarm, but thorough testing should prevent such an occurrence. In fact that's my main gripe against *VirusCure Plus*: there are simply too many annoying errors (the above description is by no means an exhaustive list), even though I liked many of the features offered by the scanner program. In short *VirusCure Plus* basically works, but it would benefit from much more testing, and needs detailed printed documentation.

Technical Details

Product: *VirusCure Plus*

Manufacturer: *International Microcomputer Security Software Inc. (IMSI)*, 1938 Fourth Street, San Rafael, CA 94901, USA. Tel (415) 454-7101. Fax (415) 454-8901. BBS (415) 454-2893.

UK Vendor: *IMSI (UK) Limited*, Unit 17, Brook Lane Business Centre, Brentford, Middlesex. TW8 0PP. Tel: (081) 758 1447. Fax: (081) 758 1667.

Availability: Not stated.

Version Evaluated: 2.32

Serial Number: None visible.

Price: £69.99

Hardware Used: A 33MHz 486 PC, with one 3.5 inch (1.44M) floppy disk drive, one 5.25 inch (1.2M) floppy disk drive, and a 120 Mbyte hard disk, running under MS-DOS v5.0.

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

PRODUCT REVIEW 2

Mark Hamilton

Trend's PC Rx

In July of last year, I reviewed *Trend Microcomputer's PC-cillin* which uses an exotic combination of hardware and software countermeasures. The company also produces a software-only product called *PC Rx*. The software is described as 'The ultimate virus protection for your PC' and 'The only anti-viral product that outsmarts all viruses, old and new, without frequent virus pattern updates!'.

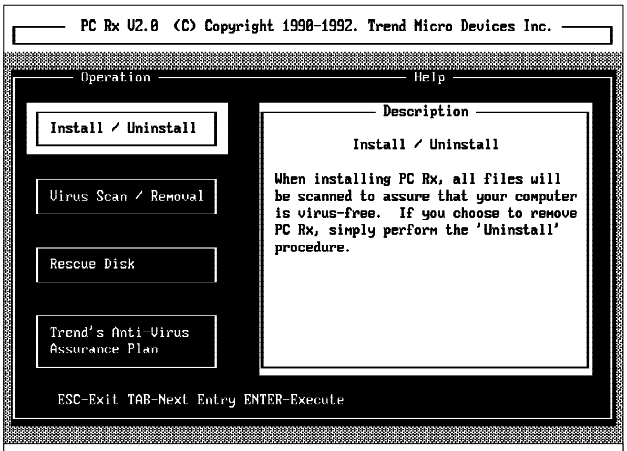
Components

Both 5.25 and 3.5-inch diskettes are supplied as standard but only the 5.25-inch disk was write-protected. The package also comprises a slim 50-page manual, a single sheet of amendments to the manual, and, a booklet entitled 'Six Important Questions About Computer Viruses.....What You Need To Know But Didn't Know To Ask' which the company published in September 1990. There is a surfeit of extraneous packing material.

The diskettes contain the following files in the Root Directory:

CHKLIST.DOC	This simply gives a directory listing of the files on the disk.
PCRX.EXE	The main program.
PCRXCFG.EXE	The configuration program for PCRXVT.
PCRXSCAN.EXE	A command-line driven virus scanner.
PCRXVT.CFG	The default configuration for PCRXVT.
PCRXVT.IMG	An installation shell which converts to PCRXVT.COM.
README.DOC	See text.
VRSLIST.DOC	A list of viruses which the product claims to detect.

PCRX is used to install (and uninstall) the software and it can also scan drives for viruses and create 'Rescue Diskettes' which contain essential information about the hard disk - such as its Partition Table and Boot Sectors. Installation is simple as PC Rx does most of the job for you. You can install to floppy or to the hard drive. For this evaluation, I chose to install to a floppy. All the programs will fit on to a bootable 360K diskette which in these days of memory- and disk-hungry applications is a refreshing change. Both memory and the disk that is to receive the software are pre-scanned for any viruses that might be lurking and then the programs are copied to the destination drive.



Installation is a simple procedure - just sit back and relax. The Uninstall routine, however, should do a little bit more than just remove the package from the AUTOEXEC.BAT file.

The installation process inserts a command to execute PCRXVT (see below) in the AUTOEXEC.BAT file - you have no choice in the matter, and once installation is complete the PC is rebooted.

As well as installing and uninstalling (which simply seems to remove the PCRXVT command from AUTOEXEC - why bother?), it also can scan for viruses using a full-screen menu. An identical scanning engine is also provided as a command-line driven program (PCRXSCAN) for the professionals who prefer a 'no-frills' approach to software security.

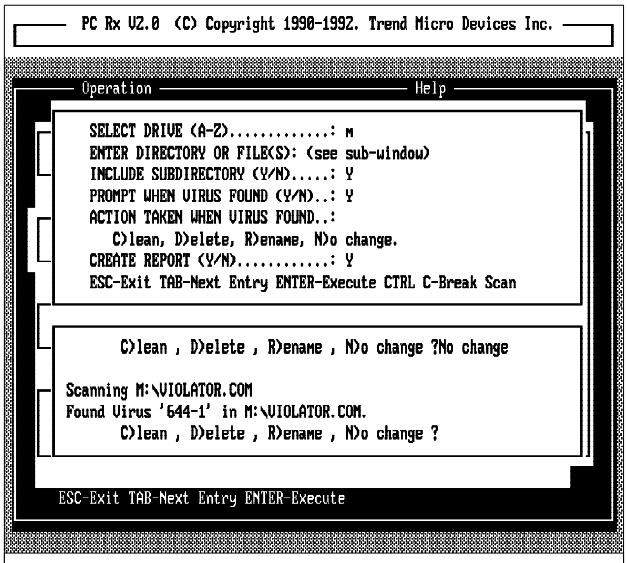
In testing, both versions scanned at the same speed and scored equally in accuracy tests (see below).

Detection

The README.DOC file boasts that *PC Rx* can detect 40 Boot Sector viruses and 1,583 File Viruses. *Trend* might claim this number, but the proof of the pudding is in the testing and this product's results are, frankly, mediocre.

Using the standard *Virus Bulletin* test set, it detected almost 93% of infections. This rating dropped to less than 74% of infections in in an unofficial 'enhanced' test battery comprising 786 infections. Using the *In The Wild* test set, it managed to detect 82% of the 116 infections, placing it in the lower end of the league table. Most notably, it missed

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

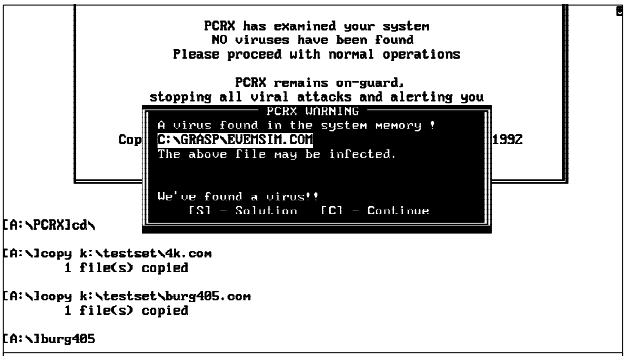


Once a virus is found there is a choice over how to proceed. The only obvious effect of the Clean option is to rename the offending file.

Nomenklatura, 8 (of 11) Whales, 4 (of 5) Spanish Telecom 1 file infections and all of the Spanish Telecom 2 samples. It fared no better in the Polymorphic test, failing to detect all samples of 1226, Evil, Phoenix and Proud.

Examining the list of viruses which the product claims to detect suggests that its authors are prone to exaggeration. As is typical with many US products, the viruses have proprietary names which conform with no convention.

Astonishingly, the package claims to detect 71 viruses with the name 'JERUSALEM(COM)', 35 called 'JERUSALEM(EXE)' and a further 33 Jerusalem samples. Somehow *Trend* has managed to find more (different?) variants of this common virus than its competitors combined. There are also 32 different Whale viruses listed, from



Gotcha! Viral activity is succesfully spotted before any damage is done. The message displayed can optionally (as in this case) be customised.

'Whale-1(s)', through 'Whale-2(s)-26' to 'Whale_6' none of which featured among the eight missed generations of Whale in the *VB* test set!

Upon detecting a virus with *PC Rx*, you are given the option of cleaning the file (i.e. removing the virus), deleting the file, or renaming the file.

However, contrary to the software's claims, 'Cleaning' the file seems to have the same end result as renaming it.

PC Rx is one of the faster scanners available - but this seems to be at the expense of accuracy. There is no distinct 'turbo' or 'secure' mode. The command-line version, PCRXSCAN provides the option to scan executables only or all files; a greater degree of flexibility is provided by *PC Rx*. *Trend* has decided that by program files, it means any file with the extension of COM, EXE, SYS or BIN - it ignores overlays (OV?) and dynamic libraries (DLL) unless these are specified either by the command line-option to scan all files or using specified extensions. It scans at a rate of 157 Kbytes per second on a 25 MHz '486. The scanner encounters problems when opening files which bear no alpha-numeric starting characters. The characters '!' or '#', both of which are legal in a file name, went unscanned, *PC Rx* refusing to recognise them.

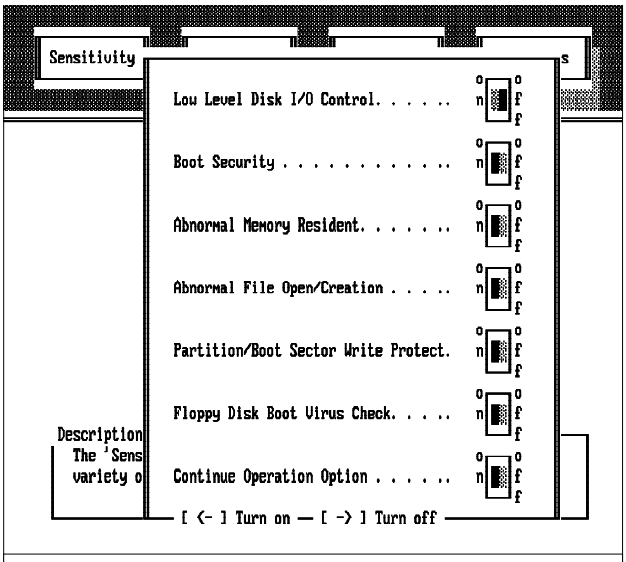
Memory-resident Protection

The second principal component of this package is a TSR program, PCRXVT. This program is started each time the PC is booted. The program monitors system activity for virus-like behaviour such as attempted modifications to the boot sector or programs. Being generic in nature, it is liable to false alarms and trips up over self-modifying programs. This program does not warn when virus-infected files are copied, which limits its usefulness. It did, however, correctly warn me that a virus was about to infect a program although the error window is completely different to that shown in the manual.

PCRXVT occupies 11,664 bytes of memory and I was unable to get it to load high using either *386^{Max}*, *QEMM* or Microsoft's memory managers when used in conjunction with *MS-DOS 5*, although *Trend* claim this is possible.

PCRXVT's options are all configured by PCRXCFG. There are four basic configurable options: Sensitivity, Display, Message and Exceptions. Under the Sensitivity menu, you can turn off selected checks that the TSR performs - the more options you disable, the less secure it becomes. As a gesture of reassurance, a visible reminder that PCRXVT is memory-resident can be invoked (a 'smiling face' character at the top right of the screen signals this happy fact). The message which appears when the TSR detects something

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.



An original and effective way of choosing how the memory-resident part of the package operates.

untoward can be customised. The 'Exceptions' menu is provided so that legitimate programs which cause PCRXVT to trigger a warning may be exempted from inspection. This option requires very careful thought prior to use.

I was surprised by the absence of an integrity checker - particularly in view of the all-embracing claims made by the product's developers. Nevertheless, *PC Rx* performed relatively better than its bigger brother, *PC-cillin* - which was bedevilled with incompatibility problems - but not as well as other similarly-priced alternatives. Considering that the test sets used have existed for some months - in the case of the 'standard test set', well over a year - I find the results of the detection tests less than I would expect from a new product hoping to break into the glutted UK market.

An important consideration is that of support. This is provided through *CompuServe* where *Trend* has an area within the *McAfee Associates* moderated virus forum. *Darele*, the UK distributors, believe that support should come from its resellers - that is to say, the dealer channel. This, I am sure, will prove insufficient.

Conclusions

This product is unremarkable - neither noticably better or worse than many of the products on the market. The detection rate is disappointing; any serious product should not miss viruses from the *In The Wild* test set. In summary, while *PC Rx* has a few nice features, it is not outstanding in any way, and, for the money, there are better products available on the market.

PC Rx

Scanning Speeds

Hard disk:		
All files	816.19 secs	
(157 Kbytes/sec)		
Executables only	206.02 secs	
Floppy:		
All files	4.50 secs	
Executables only	3.00 secs	
Test Sets		
VB Standard Test Set [1]	338/365	92%
Enhanced Test Set [2]	581/786	74%
In The Wild Test Set [3]	95/116	82%
Polymorphic Test Set [4]	110/150	73%

Technical Details

Product: *PC Rx*

Version: 2.00A

Serial Number: 1029-13DE

Authors: *Trend Micro Devices Inc*, 2421 West 205th Street, Suite D-100, Torrance, CA 90501, USA.

Telephone: (310) 782 8190.

Fax: (310) 328 5892.

UK Distributor: *Darele Associates Ltd*, Raden House, 20 Chinley Ave, Moston, Manchester M10 9HT.

Telephone: 061 682 3032.

Fax: Not supplied.

UK Price: £79.00 + VAT.

Update Frequency: Unknown and not quoted.

Test Hardware: All virus scan tests were conducted on an *Apricot* Qi486 running at 25MHz and equipped with 16MB Ram and 330MB Hard Drive. The speed tests were conducted on a *SIR* 486 also running at 25MHz and equipped with 8MB Ram and a CD-Rom drive. *PC Rx*'s scanning speed was tested against a CD-Rom containing 6,483 files (126,814,940 bytes) of which 546 were executable (30,390,671 bytes) and the average file size was 55,660 bytes. The floppy test was the same *Microsoft C v5.1 Installation Disk* used in previous reviews.

For details of the test sets used, please refer to:

[1] Standard Test Set: *Virus Bulletin* - May 1992 (p.23).

[2] This unofficial test set comprises 786 unique infections.

[3] *In The Wild* test set: *Virus Bulletin* - June 1992 (p.16).

[4] *Polymorphic* test set: *Virus Bulletin* - June 1992 (p.16).

VIRUS BULLETIN **©1992 Virus Bulletin Ltd, 21 The Quadrant, Abingdon Science Park, Oxon, OX14 3YS, England. Tel (+44) 235 555139. /90/$0.00+2.50** This bulletin is available only to qualified subscribers. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means, electronic, magnetic, optical or photocopying, without the prior written permission of the publishers.

END-NOTES AND NEWS

Alternative Computer Technology Inc has announced that ***Digital Equipment Corporation*** **has been appointed as an Authorised Reseller for *VSWEEP***, *Sophos UK's VMS*-based product for *PATHWORKS*. *VSWEEP* runs as a permanent background *VMS* job, constantly scanning *PATHWORKS* file services and sounding the alarm if a virus is found. *VSWEEP* for *PATHWORKS* therefore allows centralised, unattended, and 'stealth-proof' virus detection. For additional information call 1-800-DIGITAL, ref. Part No. QB-06FAY-W*.

IBC Technical Services Ltd is holding a one-day conference on **PC Security and Viruses** on 24th November in London. Speakers include Dr Jan Hruska and Robert Jacobson. Information from Juliet Coe. Tel 071 637 4383.

The Third Annual EICAR Conference (European Institute for Computer Anti-Virus Research) will be held on 7th-9th December 1992 in Munich, Germany. Papers will be given in German or English, with simultaneous translation. For further information contact Christoph Fischer. Tel (+49) 721 376 422.

Dr Roy Booth, a lecturer at *Newcastle University*, is in court **charged with attempting to blackmail a company by threatening to destroy a computer program** with a virus. According to a report in *The Times*, Dr Booth, who denies blackmail, is alleged to have had a dispute over money with *Imec*, of Washington, Tyne and Wear, which had hired him to develop a program. The trial continues.

PC Plus has launched ***The Virus Video*** (RRP £19.99), aimed at educating users to the risks of computer viruses. Among those featured in the video are Dr Alan Solomon, an unknown 'expert' called Edward Wilding, and Dr Simon Shepherd, of UKCVCVCL1 fame (see *VB*, July 92, p.3). Further information from *Performance Video*. Tel 08444 6682.

Currys Superstores is launching a new PC service in the UK. Using *Central Point Software's PC Tools* and anti-virus product, technicians at six ***Currys Superstores*** **will scan floppy diskettes and providing diagnostic checks on PC hardware, free of charge**. As well as providing anti-virus checks, *Currys* is now selling *Central Point Software's* products. To support the new service, *Currys* and *Central Point Software* will also provide a fact sheet which gives details on virus risks, protection, and the importance of back-ups. Information from Daine Paternoster. Tel 081 848 1414.

The *Computer Security Institute (CSI)* is holding its ***19th Annual Conference and Exhibition*** on 16th-18th November 1992 in Chicago, Illinois. The conference includes the largest computer security trade show in the United States. For information contact Patrice Rapalus. Tel 415 905 2310.

Fifth Generation Systems **has introduced toll free technical support** for the UK on all of its products. Contact Mark Horne, Tel 0494 442224.

A virus has been found on some disks sent out by *Transend Services Ltd*, a British shareware distributor. The companion virus (known as the Power Pump virus due to a text string within the code) appears to have been added deliberately to an *IQTEST* freeware package which the company distributes. A full report on this virus will be published next month.

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

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

This publication has been registered with the Copyright Clearance Centre Ltd. Consent is given for copying of articles for personal or internal use, or for personal use of specific clients. The consent is given on the condition that the copier pays through the Centre the per-copy fee stated in the code on each page.