July 1989 ISSN 0956-9979

VIRUS BULLETIN

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

Editor: **Edward Wilding**

Technical Editor: **Joe Hirst**, British Computer Virus Research Centre, Brighton, UK

Editorial Advisors: **David Ferbrache**, Heriot-Watt University, UK, **Dr. Bertril Fortie**, Data Encryption Technologies, Holland, **David Frost**, Price-Waterhouse, UK, **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, **John Laws,** RSRE, UK, **David T. Lindsay**, Digital Equipment Corporation, UK, **Martin Samociuk**, Network Security Consultants, UK, **John Sherwood**, Computer Security, UK, **Roger Usher,** Coopers&Lybrand, UK, **Dr. Ken Wong**, BIS Applied Systems, UK

CONTENTS

EDITORIAL

Technical Reviews, a comment by Keith Jackson 2
Virus Dissections, a comment by the Technical Editor 3
Viruses and Worms defined 3

KNOWN IBM PC VIRUSES 4

KNOWN MACINTOSH VIRUSES 5

CASE STUDY

A Tale of Woe from the Printing Industry 6
The n-VIR Family 7
Macintosh Anti-Virus Practices 7
Macintosh Anti-Virus Programs 7

LETTER FROM EUROPE

Hidden Virus in a Demo Disk 8
The Naughty Destroyer Program 8
Infected Continent 9

VIRUS DISSECTION

The Jerusalem Virus 10
The Fu Manchu Virus 11

TECHNICAL REVIEW

Dr. Solomon's Anti-Virus Toolkit 13

CONFERENCE REPORT

I1 Virus del Computer, Milan 15

EVENTS 16

VIRUS BULLETIN **©1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

Trend Micro, Inc.
EX1013-1

EDITORIAL

When the Brain computer virus appeared in 1986 it caused a media sensation but not an outrage. People were genuinely fascinated by the novel concept of a computer virus. Analogies started to appear in the Press; there was talk of computers catching colds, of 'data doctors' and 'vaccines' and all sorts of other jargon inspired by the world of medicine. The cartoonists had a field-day and the whole affair was widely regarded as a source of amusement rather than alarm.

Nowadays, however, wry smiles have turned to furrowed brows. Hundreds of businesses, both large and small, have suffered from the handiwork of the virus writers. It is now clear that a sabotage mentality exists and new computer viruses destroy data and programs - the more extreme examples being programmed to format hard-disks.

Computer viruses actually present a significant escalation of the weaponry available to the electronic vandal. There are a number of reasons why viruses are singularly dangerous. First and foremost is the sheer level of destruction which a pernicious virus can inflict; hundreds, even thousands, of man-hours entering essential information can be wasted in a matter of seconds and valuable, sometimes irreplaceable, programs destroyed.

Second, computer viruses replicate; the virus can spread through networks, infecting every connected workstation and thus multiplying the level of destruction and havoc caused.

Third, is the insidious nature of these programs; having entered a system the virus will provide no indication of its existence until triggered by a self-contained time bomb or a 'string' sequence is entered at the keyboard. The unsuspecting user is completely unaware that the application program he is running has infected the computer.

Finally, computer viruses reside on standard floppy disks; they can be copied and distributed widely, usually by unsuspecting people, meaning that computer viruses are capable of spreading throughout the computer-using community at an exponential rate.

Paradoxically, the drive for business efficiency and globalism serves only to increase the potential damage which computer viruses and other malicious programs can cause Unix, Open Systems Interconnection, Electronic Data Interchange, E-mail facilities, on-line databases and other datacomms initiatives are all vulnerable to attack. Indeed, the more streamlined and interconnected computers become, the greater will be the penalties resulting from carelessness, recklessness and vandalism.

Rather like Hitler's V1 'flying bomb', no-one knows when or where a computer virus will strike. They attack indiscriminately. Virus writers, whether or not they have targeted specific companies or individuals, must know that their programs, once unleashed, soon become uncontrollable. It is, perhaps, the saddest indictment of these people that they are prepared to hurt anybody and everybody.

The threat from vandalistic computer viruses already exists. There is now talk of more subtle computer viruses designed to adjust spreadsheets or accountancy packages - adding a whole new dimension to the term 'salami-fraud'.

It is with these and other dangerous computer viruses in mind that *Virus Bulletin* has been devised. We aim to provide PC users with a regular source of intelligence about computer viruses, their prevention, detection and removal, and how to recover programs and data following an attack.

Technical Reviews - a comment by Keith Jackson

Product reviews in this and future editions will cover the whole range of virus related products that are currently available on the market. I do not intend to follow the usual journalistic style of reportage followed by mild comments. This helps no-one, and can only be viewed as an offshoot of routine marketing.

It is my aim to be factual about available products, focusing on their strengths and weaknesses. It is easier to write about a particular product in neutral terms, but this does not help a would-be purchaser of this product come to a decision as to whether claims made for the product are justified.

The first product review (Dr. Solomon's Anti-Virus Toolkit) appears on page 13.

VIRUS BULLETIN **©1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

Trend Micro, Inc.
EX1013-2

Virus Dissections - a comment by the Technical Editor

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 ©**1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

Trend Micro, Inc.
EX1013-3

KNOWN IBM PC VIRUSES

Joe Hirst

The following is a list of the known viruses affecting IBM PCs and compatibles, including XTs, ATs and PS/2. If a particular virus does not execute on a 286 or a 386 machine, a statement to that effect is made in the Description section of the table. Each entry includes the virus name and aliases, its type (see the *type code* table below), hexadecimal pattern (virus signature) and its displacement within the virus and a short description of the virus and it symptoms. The hexadecimal pattern can be used to detect the presence of the virus by using any pattern searching software such as the *Norton Utilities*.

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*.

The August issue of Virus Bulletin will contain a dissection of the Datacrime (1168) virus. Full details about its detection and removal will be included. Also, a preliminary report on Traceback (3066) virus, a detailed dissection to follow in September.

VIRUS BULLETIN ©**1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

Trend Micro, Inc.
EX1013-4

KNOWN APPLE MACINTOSH VIRUSES

David Ferbrache

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

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

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

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

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

Characteristic byte sequences: (from Virus detective Ver 3.0.1)

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

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

VIRUS BULLETIN **©1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

Trend Micro, Inc.
EX1013-5

CASE STUDY

John Sherwood

A Tale of Woe from the Printing Industry

This case study concerns a printing firm wrestling with the difficulties of introducing new technology. Amongst other troubles they have suffered TWO virus infections.

The company is small, but with a well established business and a good reputation for the quality of their work. They employ fifteen people and print a wide variety of items, many of which involve high-quality, multi-colour printing with a gloss finish. They handle a lot of brochures and some glossy magazine printing.

To remain competitive they have had to introduce electronic typesetting and desk-top publishing.

The computer technology used by printers is of the most advance variety, including very high-resolution colour screens and laser printers with custom bit-mapped fonts. This company's configuration comprises three Apple MAC II workstations connected together on a TOPS local area network, sharing a LaserWriter II and a Linotronic 300 typesetter. One of the Apple MAC IIs also has a serial connection to a Linotype Workstation 2000 running MS-DOS.

The entire configuration is supplied and supported by Linotype. Applications software in use includes desk-top publishing (PageMaker and Quark-Express) and word-processing (MS-WORD).

The first brush with viruses came when Linotype delivered the equipment, but unfortunately did not ship the software. The installation engineer discovered this deficiency only the day before the customer training representative was due to come and show them all how to use it. There wasn't time to get the software that should have been shipped, so they contacted the local Apple dealer. The dealer made some copies from their own demonstration system. There were installed by the engineer and the system was up and running in time for the training session.

When the customer trainer started to use the system, she diagnosed a virus. Hurried arrangements were made whereby Linotype shipped the correct software and the problem was cured. The company was a little dismayed by the hiccup, but everything seemed to have been put right.

Printing firms that have sophisticated plant often offer a bureau service to others who want to make use of the facilities. One such client of this company wanted to use the Linotronic 300 typesetter to get the level of definition required for a particular job. The problem was that although the job to be run off was under PageMaker (and that was available on the system), it also made use of a graphics package called ILLUSTRATOR, which was not available.

"Never mind", said the client, "I've got ILLUSTRATOR, so I'll bring it along and we'll install it on your system. Then we can use my software to drive your typesetter."

After the client had left, they needed to take the system down for some minor systems administration, but they couldn't boot up again! All their typesetting work was held up. It didn't take long to register that the problem was probably caused as a result of something done by the visiting client. They invited him to come back and sort out the problem.

As he failed to overcome the difficulties, he contacted a friend who worked in the computer science department at the nearby Polytechnic. He was familiar with Apple MAC viruses and quickly diagnosed this one as n-VIR. A program called "Disinfectant" (Version 1.0, March 19 1989, John Norstad, Northwest University, USA) was supplied which cleared up the symptoms and everything worked again. Shortly afterwards the service engineer called, and gave them another programme called "Virus detective" (Jeffrey S. Shulman, Ridgefield, CT, USA). This program reported that the system was still infected and offered to clean it up. Since then they have been operating without problems, except the worry of how to offer a bureau service without catching a nasty cold.

For information on the n-VIR virus see tables on page 5 and opposite.

VIRUS BULLETIN ©**1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

Trend Micro, Inc.
EX1013-6

The n-VIR Family

The ubiquitous n-VIR has spread throughout the Macintosh world. It is a complex virus about 3.4 Kbytes in length, with at least five variants most of which are benign producing the occasional beep or “Don’t Panic”. The virus spreads from any infected application run into your hard-disk or floppy system file. A system booted from an infected system file will infect any application run (including finder). Keep an eye open for changes in file alteration times. To confirm use Resedit to look for resources of type n-VIR, Hpat, AIDS or MEV# in applications and the system file.

Macintosh Anti-Virus Practices

1. Don’t run foreign software from unknown sources

2. Watch for unusual behaviour - system bombs, strange disk activity, printing failures, changes in file alteration times, notepad and scrapbook files are documents not Macs, messages when locked disks are inserted, slowdown in starting applications etc.

3. Add in INIT to your system folder to trap attempts by a virus to add code to the resource fork of applications.

4. Periodically run a virus search program over your hard and floppy disks.

5. Always write protect your system and utility floppy disks.

6. Take regular backups - not just one set - many viruses have long incubations periods!

Macintosh Anti-Virus Programs

INITS to prevent virus propagation:

Vaccine Ver 1.0.1	Simple protection for application users
Gatekeeper Ver 1.1	Configurable to allow development work
Warning	Low profile protection for programmers

Utilities to search for viral code in applications or system files:

Virus detective Ver 3.0.1	Configurable desk accessory
	Can auto-scan floppy disks under multi-finder
Disinfectant Ver 1.1	Best shareware search application
	Finds all confirmed Mac Viruses
Virus Rx Ver 1.4a2	Apple’s own anti viral product
Interferon Ver 4.0	Updated version of the old favourite

Make sure you are running the most recent versions. Old versions don’t recognise the newer AIDS, MEV or anti viruses.
The latest versions will be available on the MacUser anti-viral disk, MacUserware, PO Box 320, London N21 2NB; or by electronic mail from the comp.virus archive site at info-server@uk.ac.hw.cs

VIRUS BULLETIN **©1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

LETTER FROM EUROPE

Hidden Virus in a Demo Disk

During a data security conference held in May by the Unione Industriale di Torino of Italy a consultant from Tel Aviv, Mr Gabriel Vago, gave an example of a recent malicious virus propagation in Israel. The virus program was designed to attack microcomputers, and its aim was simply the creation of a demand for anti-virus software.

After the infamous Jerusalem virus had cause wide-spread concern in Israel, a software company developed an anti-virus program which was marketed to a number of potential clients. Most of those approached about the product declined to take it believing the virus threat was not serious enough to warrant it. However, a second approach by the vendor soon followed.

A seemingly attractive graphics package was offered to the same list of people who had received information about the anti-virus software. Included with the descriptive literature for the package was a demo diskette which showed some of the features available on the actual product. Within days telephone calls were being received by the vendor from people who had used these demo diskettes. They urgently needed the anti-virus package because something was spreading over hard-disks, blocking systems, and causing damage and denial of service.

There was, of course, suspicion that it was the demo diskettes which had caused these problems. Subsequent examination of the graphics packages, however, showed no sign of virus code or any other infecting function.

Following a number of incidents of infection, one of the users who had received the graphics diskette used some utilities to examine it without running its program. The truth then became apparent. The graphics demo diskette did include a computer virus which had, among other functions, a routine which enabled the virus to wipe itself out once the hard-disk was infected.

Hans Gliss

The Naught Destroyer Program - A Little Nightmare but not a Virus

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 ©**1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

Trend Micro, Inc.
EX1013-8

Infected Continent

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*.

"Nurses used to play an infected copy of Leisure Suit Larry on the patient status registration system. A potentially lethal scenario!"

VIRUS BULLETIN ©**1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

Trend Micro, Inc.
EX1013-9

VIRUS DISSECTION

Joe Hirst

The Jerusalem Virus

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 **©1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

Trend Micro, Inc.
EX1013-10

VIRUS BULLETIN ©**1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

Trend Micro, Inc.
EX1013-11

VIRUS BULLETIN ©**1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

Trend Micro, Inc.
EX1013-12

TECHNICAL REVIEW

Dr. Keith Jackson

Dr. Solomon's Anti-Virus Toolkit

The stated aim of the anti-virus toolkit is to provide accurate information about viruses, details of how they work, and a set of computer programs (tools) useful for dealing with the virus problem. It is published by Alan Solomon who has kept a very high profile with regard to computer virus infections. This review concentrates on one particular aspect of the anti-virus toolkit, as well as giving an overall impression of the facilities offered by the toolkit.

The software comes on a 5.25 inch floppy disk with no write protect notch. Therefore programs cannot write to this disk. A write protect tab could conceivably be removed. Not having a write enable notch on the disk in the first place is an excellent precaution, when you think that the programs are intended to be used in a situation where viruses may be writing surreptitiously to disk.

The software in the toolkit splits into three distinct types. Programs whose main function is to detect and eradicate viruses, programs which aim to help the user manipulate disks and/or files, and programs that try to prevent virus activity once infection has taken place.

First the programs that locate and eradicate viruses. Programs are included which can detect file changes which may be caused by a virus, search for known viruses on a disk, remove known viruses, and overwrite either a file or a sequence of bad sectors (either of which can be hiding a virus). These programs are the best art of the anti-virus toolbox.

From my own testing they all work, though the user interface could well be improved somewhat. There are however some limitations. The program called FINDVIRUS looks for known virus "signatures" by searching for sequences of bytes known to exist within current viruses. It has the obvious, and insurmountable, limitation that it can only check for viruses that are currently known to exist. It is also very slow. I measured search rates of 11 Kbytes per second on a 3.5 inch floppy disk, and 22 Kbytes per second on a hard disk.

The second of the three types of program available in the toolkit are those concerned with disk an/or file manipulation. Programs are included which can undelete files, permit a user to inspect parts of a disk at a low level, and examine a file in either ASCII of hexadecimal format. Without exception these utilities have an unforgiving user interface, and error reporting can only be described as minimal.

The programs that aim to prevent virus activity offer facilities which can prevent all disk writing (a kind of software write protect feature), and "inoculate" a disk to prevent a virus replicating itself on to the disk.

These come into their own if you already have a virus outbreak. For instance, preventing all disk writes does not exactly blend in with actually using a computer. Sooner or later you are going to need to write to disk to actually do some work. However this kind of write prevention is extremely useful whilst working on an infected system. It worked quite well when I tested it.

Many viruses inspect a disk to see if a copy of the virus is already present before they replicate themselves and infect the disk. If they did not do this, each disk could become multiply infected to such an extent that the system became unusable. Such a strategy does not help a virus to survive. On a virus-free disk, an inoculation program writes the bytes sequence which the virus tests to see whether the disk is already infected. In future, the disk will appear to be already infected, and the virus will not try to infect the disk again.

Specific inoculation programs are provided against the following viruses: *Brain, Italian, Stoned, 648, 1813, 1701, 1704* (these are the names as specified in the documentation, please see page 4 for aliases). Inoculation of all disks is not a strategy to be used unless a virus outbreak is already known to be present, in which case it is a precaution that can help to ensure that every single copy of a virus is eradicated. Remember that whilst removing a virus infection, you only need to leave one copy of the virus behind, and the outbreak could recur.

The method of checking whether any part of a disk has been altered by a virus (CHKVIRUS), exhibits problems with the algorithm used to calculate the checksums for these files. Details of this algorithm are not disclosed by Alan Solomon. To prevent reverse engineering by a particular clever virus, such an algorithm must be cryptographically strong. If it is not,

VIRUS BULLETIN ©**1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

it may be possible to deduce the algorithm from inspecting checksums and/or files.

I decided to try and work backwards and derive the algorithm used by CHKVIRUS simply by inspecting the checksums produced from various files. To my surprise, this proved possible after only three hours work. At the end of this time, I had derived how the CHKVIRUS algorithm works, and written a program capable of accepting a filename, reading the contents of the file and calculating the correct checksum. It seems to work for any file.

Remember that I began with no details of how the algorithm works (it's a secrete algorithm), and found no need to disassemble any program in the toolkit. I make no claims for any particular mathematical skills in figuring out the secret algorithm used by CHKVIRUS to calculate a checksum. It is trivial in the extreme, don't use it.

There is a balance that must be struck between cryptographic strength (which is essential), and speed of execution (which is extremely desirable). If CHKVIRUS is going to be executed every time that a computer boots up, then it is essential that it is capable of checking the relevant portions of the hard disk fairly quickly. If the check takes many minutes to perform, then nobody will use CHKVIRUS. A simple algorithm executes quickly.

There are other products on the market offering checksum schemes using algorithms that are known to be cryptographically strong, but they can suffer from the aforementioned speed problem. For instance I've previously tested Vaccine from Sophos which offers a mode where all checksums are calculated using the ISO authentication algorithm. I'm on record as stating that this mode is too slow to use routinely.

There is no simple solution to the problem of speed of execution versus cryptographic strength. A balance must be struck, but the algorithm used by CHKVIRUS is not the way to go. It can be reverse engineered. To release the specific details of this algorithm would be irresponsible. It is a secret algorithm, and publication may harm the users of the product. However I firmly believe that discussion of such weaknesses can only improve matters, by ensuring that stronger algorithms are used.

As proof that reverse engineering is possible, a compiled program capable of mimicking the checksum calculation process used by CHKVIRUS is available from the author of this article. If you are interested in a copy, just send a blank floppy disk and return postage to *Virus Bulletin* with a note explaining that you would like a copy. This disk does not reveal how the algorithm works, it just proves that CHKVIRUS can be (and has been) reverse engineered.

In conclusion, if you think you may already have a virus outbreak, the anti-virus toolkit offers excellent explanations of what to do, and a comprehensive set of programs in the virus specific portions of the toolkit. The parts of the toolkit that provide facilities for inspecting disks are frankly terrible. Buy a copy of one of the utility packages such as PC-Tool or the Norton Utilities. They offer many more facilities, and when combined with the virus specific sections of the toolkit offer what is probably one of the best combinations currently available to fight a computer virus infection.

Because of the problems with the algorithm described above, I cannot recommend using the CHKVIRUS program to detect whether a virus has altered any part of a disk. However such a cautionary note does not apply to the other parts of the anti-virus toolkit. If you intend to try and cure a virus infection yourself, or if you want to learn nitty gritty details about viruses, then the anti-virus toolkit is good value for money at £49, and should prove a useful purchase for any reasonably computer literate person wanting to start to deal with a computer virus infection.

Developer and Vendor: S&S Enterprises, Weylands Court, Water Meadow, Germain Street, Chesham, Bucks HP5 1LP (Tel. 0494 791900).

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

Version evaluated: v2.2, serial number T00863.

Price: £49, one-off price.

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

VIRUS BULLETIN ©**1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

CONFERENCE REPORT

Dr. Jan Hruska

II Virus del Computer: Analisi, Prevenzione, Difesa, Milan, Italy, 9-10 June 1989

The title of this conference hardly needs translating. Organised at the Milan permanent exhibition grounds (Fiera di Milano) by SMAU and the Milan University Information Science Department, it addressed the topic of computer viruses. The conference was **completely free** and some 250 people attended.

The delegates' folder handout comprised the usual summary of the papers (Italian and Inglish), a short booklet 'Report sul Virus del Computer' (in Italian) and demonstration disk for IBM-PCs donated by Monadori Informatica. I was somewhat surprised that free software should be given away at a computer virus conference, but the organisers obviously did not see anything wrong with that.

A number of Macintosh computers were available to delegates, running a rudimentary, but graphically perfect, tutorial explaining various terms used in the study of viruses.

The welcome speech by Enore Deotto was followed by a presentation by Edward Fredkin, Boston University. He spoke of 'Life, Science, Software, Computer Virus' and pointed out that the computer virus is only the first manifestation of a living organism inside the computer. 'In future', he said, 'we are likely to see other forms of computer life'. Trying to dispel the image of the virus as something evil, he proposed that we should stop complaining and talking about them, and start working.

Giancarlo Martella, Professore Stradordinario for Corporate Processing in the Information Science Department of the Universita degli Studi of Milan provided a definition of a computer virus and touched on how to combat them. He tried to make the presentation digestible for everybody by not going into technical details.

Dr. Harold Joseph Highland spoke next and proceeded to give a live demonstration of a number of Trojan horses and viruses, including a virus written entirely in Lotus 1-2-3 macros. Professor Highland can normally scare the living daylights out of any virus-sceptical executive. Not surprisingly, he managed to do so this time as well, and stimulated the discussion which followed. One of the questions to the panel concerned the inside information about the 'Virus della pallina', or the 'Italian', as it is known in English speaking countries, and which may have been available to the panel. The panel did not have any, but Marco Mezzalama for Turin Polytechnic said that since 1982 they have had a large PC laboratory where students could experiment with PCs. Over the years, he had a number of student who were capable of writing the virus, but to his knowledge, they did not.

Antonia Anselmo Martino, professor of Political Science of Pisa University explained that Italian law does not offer any protection to the virus victim. Martino's main message was that since the law will not protect you, use the means at your disposal to protect yourself.

The second day was even more crowded than the first. Marco Mezzalama, Professor of Computer Science at Turin Polytechnic opened the proceedings with a paper on 'Organising the fight against viruses'. This was followed by Keith Bostic from Berkley Computer Systems Research Centre who gave a very good presentation on the hunt and extermination of the Internet worm which infected 10,000 machines in 5 hours. Apparently, at 7 pm on the fatal day Berkley itself was infected, By 1 am they managed to find the offending bug in Unix and fix it. That stopped the worm from spreading, and by 3 am the Unix bug fix was posted to other users. Acknowledging the difficulty of combating viruses he gave the reasons: 'There are not secrets: for example, everybody can see Unix source codes. Furthermore, potential attackers have access to machines, both running Unix as well as PCs. Lastly, user convenience is intruder convenience'.

Paolo Crosignani of the National Institute for Tumors in Milan was next to perform. He drew analogies between biological growth and computer viruses, biological vaccines and computer anti-viral products. 'Can medical epidemiology help in understanding the diffusion of computer viruses?' he asked.

The round table which concluded the conference proceedings had the benefit of wisdom of representatives of big computer companies like Olivetti, Apple and IBM.

VIRUS BULLETIN ©**1989 Virus Bulletin Ltd, England. /89/$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 or a licence permitting restricted copying issued by the Copyright Licencing Agency.

Trend Micro, Inc.
EX1013-15

EVENTS

IBC Technical Services is holding two consecutive one-day seminars. On 29 June 1989 the subject is **Computer Viruses** and the following day there is a **PC Security seminar**. Both events take place at the Marriott Hotel, London. Details from Carol Gerrard at IBC, UK, Tel 01 236 4080.

Sophos Ltd is holding a number of *Computer Virus Workshops*. The next ones are on 25 July 1989 and 26 September 1989 and are held in London. Further details from Karen Richardson at Sophos, UK, Tel 0844 292392.

Datapro is holding a one-day seminar on **Logic Bombs, Trojan Horses and Computer Viruses**. It takes place in London on 12 September 1989. Details from Rosemary White at Datapro, UK, Tel 06828 773277.

Compsec '89 in conjunction with the EDP Auditors Association Annual Conference includes a special presentation on the computer virus threat. The event takes place at the Queen Elizabeth II Conference Centre, London, from 11-13 October 1989. Full details from Penny Moon, Elsevier Seminars, UK, Tel 0865 512242.

The Annual Brief on Secure Systems, 29-30 November 1989, Amsterdam, The Netherlands. For details contact Peter Hoogenboom, the Netherlands, Tel +31 3403 79597.

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

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

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, PO Box 875, 454 Main Street, Ridgefield, CT 06877

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.