ISSN 0956-9979 OCTOBER 2000

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

Editor: **Francesca Thorneloe**

Technical Consultant: **Matt Ham**

Technical Editor: **Jakub Kaminski**

Consulting Editors:

Nick FitzGerald, Independent consultant, NZ
Ian Whalley, IBM Research, USA
Richard Ford, Independent consultant, USA
Edward Wilding, Maxima Group Plc, UK

IN THIS ISSUE:

- **Anniversary edition:** a slightly different look to this month’s *Virus Bulletin* is explained on the news page. Indulge us, won’t you?
- **Stream of abuse?** Dismiss it out of hand or hype it up, the W2K/Stream virus is new and fairly unusual. Péter Ször takes a look on p.6.
- **Hello hybrid:** Igor Muttik explains the investigatory procedure he applied to a new virus which looked all too familiar but which proved to be altogether strange, on p.7.

VB2000 TENTH 10
Florida ANNIVERSARY

CONTENTS

COMMENT

NEWS

VIRUS ANALYSIS

VIRUS CASE STUDY

FEATURES

PRODUCT REVIEW

VIRUS BULLETIN **©2000 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. www.virusbtn.com /2000/$0.00+2.50** No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

COMMENT

“ … we’re always ahead of the main feature. ”

Caffeine and Cover Stories

August 1997’s *VB* had a new Editorial Assistant. Pulitzer prize-winning it wasn’t but my name was still in print. With such reliable back-up as Jakub Kaminski, Ed Wilding, Richard Ford and Ian Whalley, my biggest challenge was to decipher what my new boss was telling me. Don’t get me wrong, it wasn’t the antipodean twang, or even the mesmerisingly meandering sentences that were to characterise an editorial era – this was pure techno-speak. Nick FitzGerald was so damned qualified – all I had to do was watch, listen and not pull out any plugs. Oh and produce an eye-watering espresso every ten minutes.

That issue makes me shudder. Who spelt Nachenberg with a ‘u’, and why did my first front cover lead with ‘Errata’? Content-wise it set some fairly routine precedents: in the news, a major AV company was embroiled in some kind of legal action; the Editorial suggested that ‘the number of known macro viruses will more than double in the last six months of 1997’, and Cap topped the prevalence table. Privately, the dear old monthly *IBM* PC virus update was bringing me out in a rash and my cappucinos resembled toxic waste, but I was too busy to care. My job was to pull out of a whirling washing machine of rumour, conviction, waffle, confirmation and conjecture a clean, pressed and sweet-smelling 24-page journal for the discerning user. All this without soiling our relationship with the AVers while simultaneously passing the subscriber doorstep challenge that *VB* is whiter than white. To this day, a stray red sock will occasionally get as far as the spin cycle.

By October I was punning in the headlines, ad libbing the news and forgetting to wince when I called to talk to ‘Eugene’ instead of deferring to ‘Mr Kaspersky’. A month later my burns were healing nicely. My baptism of fire at VB’97 in San Francisco marked my first up-close impression of ‘the AV industry’. I remember clocking the cautious solidarity between this band of brothers (and sisters, but that was an observation I was discouraged to analyse). A palpable tension keeps it dynamic – deep mutual respect sits uncomfortably with flashes of occasionally grotesque show-manship but at least I was able finally to dispense with the myth that AV is a minnow tagging along with the sharks of computer security. I appreciated for the first time the high regard in which *VB* is held – on that day I started to think of my humble occupation in terms of obligations and minimum standards. I also started to smoke again, but that may be unrelated. The rest I remember like movie previews – with some of the best brains in the industry forecasting for us, we’re always ahead of the main feature. In October 1998 we trailered network-aware malware; we screened VBS viruses and email worms before they topped the bill; we premièred the fall of *PowerPoint*, and *Access* and Java… Unsurprisingly, we’ve just sent the Liberty Trojan for PalmOS straight to video.

Tired of walking on eggshells as far as certification went, we cracked some free range into the VB100% awards scheme in January 1998 – and we’ve been pelting the AV marketing departments with the leftovers ever since. When, four months later, Editorial Assistant became Assistant Editor I finally succumbed to the obsession with Columbian fresh roasted. The news pages that month profiled a petty criminal called CIH which by August was one of PC’s least wanted. By November 1998 I was so at home that I blithely published a photo for which Carey still hasn’t forgiven me and got stuck into that season’s heated debate about the *WLO* supplying AVers with virus samples. When I took over as Editor in March 1999, I was sure enough of my ground to venture off-piste and hit fresh powder. As Melissa hit we started the ‘Day in the Life’ column, the Comment page followed and the hugely popular relaunch of the Letters pages kicked off in June 1999. 2000 saw archive file detection implemented in reviews and the promise of a Mac Comparative soon. My best memories are simple ones: opening VB’99 in Vancouver, getting carolling penguins past the proofers in December, thank yous from better and better informed subscribers, catching the news before print, and most of all the frequent, satisfying clang of the buck stopping up against my size fours. I’m proud of two things; maintaining *Virus Bulletin’s* reputation as a watch-dog not a lap-dog, and not lighting up for a year. Iced decaf latte mochacino? No problem.

Francesca Thorneloe, Editor

NEWS

Happy 10th Birthday

We make no apologies for the unashamedly sentimental tone of this edition. *Virus Bulletin's* conference is ten years old and we're celebrating along with the names that have made this magazine the respected industry standard that it has become.

Ex-Editors and members of the Advisory Board were asked to contribute their thoughts to this very special issue. We feature those who responded, along with the year in which they joined *Virus Bulletin*, remembering the hows, whens and wherefores behind the magazine and its inexorable evolution. As is traditional, and in our opinion healthy, some of them do not see eye to eye on the basics …

Pressing Concerns

Virus Bulletin recommended milk and cookies all round as the playground-style scrapping of the AV industry reached its peak this week. *Kaspersky Lab's* press office, clearly working overtime lately, put out a sulky release denouncing its AV chums as unethical detractors and justifying its latest round of media – labelled hysterical by several competitor companies – about the potential dangers of NTFS and ADS.

While it is mildly amusing to gauge who gets the most negative publicity from tit-for-tat squabbles like this – does it really help the users? In our opinion, inter-industry tiffs such as this, and their inevitable repercussions, serve only to confuse and obfuscate

100% Fantastic

Well, this is new – another VB 100% award infringement, but with a difference! In fact, *Virus Bulletin* didn't know whether to chastise or commiserate with German firm *GDATA*, whose creative use of the logo adorning the Dutch version of their *AntiVirusKit2000* was nothing short of a marketing mess.

For a start, we can confirm that we have never reviewed this product in the magazine, either in a standalone or a comparative test. That didn't seem to be a problem though, and then we discovered why – *AVK2000* uses the *AVP* engine. Clearly the chaps at *GDATA* consider this to be a sufficient validation of the use of *AVP's* VB 100% awards. But it doesn't stop there.

The usual claim of '100% active virus detection' was almost forgiven, but when we looked closer and saw a VB100% award from February 1998, as presented by 'London-based Virus Bulletin' we started to wonder – a two year-old ItW virus detection award it didn't win from a mythical company which doesn't exist – just who are *GDATA* trying to kid?

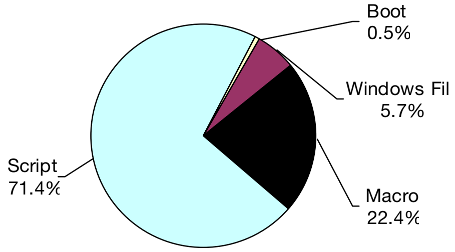
Prevalence Table – August 2000

Virus	Type	Incidents	Reports
LoveLetter	Script	577	33.6%
Stages	Script	470	27.4%
Kak	Script	177	10.3%
Laroux	Macro	91	5.3%
Win32/Ska	File	59	3.4%
Marker	Macro	49	2.9%
Divi	Macro	38	2.2%
Barisadas	Macro	34	2.0%
Class	Macro	33	1.9%
Win32/Pretty	File	30	1.7%
Tristate	Macro	27	1.6%
Thus	Macro	22	1.3%
Assilem	Macro	17	1.0%
Ethan	Macro	17	1.0%
Myna	Macro	11	0.6%
Cap	Macro	9	0.5%
Melissa	Macro	9	0.5%
Story	Macro	6	0.3%
Win32/Fix	File	6	0.3%
VCX	Macro	3	0.2%
Win95/CIH	File	3	0.2%
AntiCMOS	Boot	2	0.1%
Form	Boot	2	0.1%
VMPCK	Macro	2	0.1%
Wazzu	Macro	2	0.1%
Others[1]		20	1.1%
Total		**1716**	**100%**

[1] The Prevalence Table includes a total of 20 reports across 20 further viruses. Readers are reminded that a complete listing is posted at http://www.virusbtn.com/Prevalence/.

In order to avoid a distortion of the figures, data for the 'self-reporting' W97M/ColdApe virus (totalling 702 reports in August) have been omitted from the table this month.

Distribution of virus types in repor



LETTERS

Dear Virus Bulletin

Small Reflections

Congratulations to *Virus Bulletin* for reaching its tenth anniversary conference as my son celebrates his fourth birthday.

My life will forever be intertwined with each *VB* conference with the stark memory of stepping into my room at the Grand Hotel in Brighton and seeing a note on the floor. It's too bad I didn't keep that note for a souvenir. For those who weren't at Brighton or somehow missed the opening sentence, that note was from the hotel management informing me that my wife had gone to the hospital. By the time I called, I was the proud papa of my second son, Matthew, my third and youngest child.

Matthew is growing, learning, and a fantastically energetic boy, as I see the annual *VB* conference also getting bigger and better each year. I hope however that it never loses the charm and warmth of the earlier years. The warmth and kindness and congratulations I received from everyone at the conference is forever etched into my memory, though I wonder how well Kim and Paul appreciated that bottle of champagne.

So, with every *VB* conference upcoming, I will have fond memories, starting with Edinburgh, to having the honour of the keynote address, through Vancouver, and on to Orlando.

'Happy Birthday' – *VB* will always be so special, …and many more.

Jimmy Kuo
Network Associates Inc
USA

Adventures in Head Hunter Land

Each and every international *Virus Bulletin* conference and exhibition offers a wealth of opportunities – meeting top AV people, hearing timely and useful presentations, and (if you work in the industry) getting lots of job offers. Indeed, many of my fondest memories (and a couple of jobs) originated at *VB* conferences.

VB and I sort of grew up together. I received and analysed my first virus just one month after the first issue of *VB* was released. However, being just a lowly virus deprogrammer, I didn't get to attend the first few conferences. In 1993 I was invited to join the Advisory Board by Richard Ford (it was at a *Virus Bulletin* conference; I introduced Richard to Sarah Gordon, now his wife).

My first *VB* conference was in 1994 in Jersey (the one off France, not the one off Philadelphia). At that conference I presented a paper on (surprise!) 'Viruses in the Wild' and got two great job offers. Upon returning to the colonies, I soon after left the *Peter Norton Group* to join the AV team at *IBM's Thomas J Watson Research Centre*. Then, when I left *IBM* I followed up the other lead and accepted Pete Radatti's offer to join *CyberSoft*.

At the 1996 conference, I introduced Shane Coursen to anti-virus people. He outdid me by receiving five job offers. Soon after he left the *Peter Norton Group* for the *Alan Solomon Group*. Now that I think about it, I believe it might be mathematically provable that the two most common ways of changing AV employment are by (1) corporate acquisition and (2) *VB* conference attendance.

But even if you're not looking for work, *VB* is a great place to be. Where else can you pester *CAI* sales reps with esoteric techie questions? Where else can you sit between Graham Cluley and Nick FitzGerald while kibitzing at Vesselin Bontchev's presentation? Where else can you learn so much about viruses while having such a good time? Nowhere. That's where. And who knows? You might even get a job and a spouse.

As a board advisor, my advice is simple. Be there, have fun, and if you work in the industry, bring several copies of your resumé and give me a copy before you give it to anyone at *Symantec*, *NAI*, or *Trend*.

Here are some trivia questions from past *Virus Bulletin* conferences:

- Which *Symantec* employee was put in a guillotine?
- Which conference director was put in a straight jacket?
- Which AV person made a laughable attempt at juggling and mime on stage?
- Which AV person's wife stole the most balloons at a gala dinner?
- Which two AV people fell off the stage during their presentations?

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

- Who wore the 'Die Yuppie Scum' hat with a built-in ponytail?
- Which (former) *Dr Solomon's* employee was photographed in an *IBM* AV shirt?

Joe Wells
WarLab
USA

Part of the Team

I was just looking inside some *Linux* binaries and once again reached for a copy of my i486 manual. How many times have I browsed through these once immaculate, snowy white pages, now held together with bits of sticky tape? Publication date: 1990! Covers bent, corners missing, so used and battered, and still so useful and so much needed. Could this symbolize the last ten years of the AV industry? Undeniably so.

I have no doubt, the AV industry has grown up and has reached its maturity. The sins of youth have been left behind along with the feelings of absolute righteousness and omnipotence. Adulthood brought the experience, knowledge, expertise and confidence of a long distance runner. However, it also introduced its small compromises, corruptions, corporatizations, bitterness and questions about the future. Seems like the right time for a midlife crisis.

So, where do *Virus Bulletin* and especially the *VB* conferences stand in all this? I'm not going to present you with an unbiased opinion here, because it's impossible. My personal involvement in *VB* affairs are too deep to guarantee an unspoiled objectivity. Like Sarah (p.16), Jersey 1994 was my first *VB* conference. (I thought the late night fire alarm in the hotel that year, was part of the promised entertainment.) There, I watched and listened to people whose names and works I had been learning since 1992. I was fortunate that the culture of the company I was working for encouraged research and an international presence.

The next year, I was the fresh Technical Editor and I joined the crowd as one of the speakers. If you are not a native English-speaking person and have a chance to stand in front of the élite of AV researchers and high profile users, you will understand what I went through. But one of the great things about the *VB* conference is that it is truly international; speakers and participants come from all over the world. It is an event where knowledge and competence is what really counts and I believe the overwhelming reason for its growth and success. Various AV industry official and informal bodies schedule their regular meetings at the VB conference, since the venue guarantees the presence of a significant number of their members. These, along with the social program, other out-of-session activities, and endless discussions over lunch and coffee make the conference a kind of AV endurance test.

By convening this year's event in Orlando, the organizers have broken their own, unwritten but almost sacred rule which has helped to keep the participant numbers high – for the last six years, each conference was held in cities of different continents, alternating between North America and Europe. We can expect riots, and I see Pavel's post-script (p.15) as a clear warning. Moreover, I know of a growing Antipodean lobby which will demand that the outcome of the vote held at the end of San Francisco conference in 1997 be upheld.

The chosen countries and cities are never a disappointment. But what makes the conference stand out is the organization and attention to detail from start to end. The session rooms are always well set-out; the audio-visual specialists and the organising team ensure that the delegates get their value and are able to participate in the question time at the end of the presentations. And don't forget about voluminous and always up-to-date conference proceedings. (Those of you who had the questionable pleasure of taking part in a certain conference in New York, in March 1993, will know what I mean. And the picture of two speakers trying to deliver their papers at the same time, from the same stage is still haunting me to this day – that was the very first computer security and virus related venue I'd ever been to.)

All of the above reasons make the tenth *Virus Bulletin* conference a great occasion for me. I've been very lucky and very honoured to be closely associated with the organization over the past five years. Being a part (even a relatively tiny part) of the *VB* team is something to be proud of. If all goes as planned, this will be my seventh consecutive *VB* conference, sixth as a speaker. Last year the schedule was just perfect, but this year I have a bone to pick with the organizers – being scheduled to deliver the presentation on Friday (*pardon le mot*) sucks! It's almost like saying to a speaker: 'no fun for you on Thursday night!'. But I guess I shouldn't complain, I could be in Vesselin's or Robert's shoes.

One more thing, I've almost forgotten I was supposed to keep this piece technical for the benefit of, as I was instructed, *heartless people like myself*. Let's try – there has been an opinion lately that users should stop using anti-virus scanners. All I'd like to say to those who are ready to ditch their scanners is: hold on just a little while longer. Before you make a final decision, read at least the closing sentences written by Ray Glath (p.10). It is true, and as soon as we find this 'better way', I'll be the first one to drop my scanners.

Jakub Kaminski
Virus Bulletin Technical Editor

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

VIRUS ANALYSIS

Stream of Consciousness

Péter Ször
Symantec Corporation

In September, Benny 29A and Ratter released W2K/Stream, the first known virus to utilise NTFS streams. The virus (and the surrounding hype) generated much confusion for users worldwide. This is understandable. Currently most (all?) on-demand anti-virus software does not scan the NTFS streams for virus code. Since NTFS streams are invisible with standard *Windows NT/2000* applications the news generated panic among users, just like when NTFS streams were first discussed in public (at the time without an actual virus example).

In recent news some 'experts' went as far as claiming that systems will be 'Trojanised by current AV software'. In this short article I do not intend to comment on all the false claims. However, I would like to say that as far as the detection of the virus is concerned, it should be no problem for any current AV software.

W2K/Stream uses an NTFS feature that exists on both *Windows NT* and *Windows 2000*. The virus writers believed that this particular feature did not exist on *NT* and reduced Stream to being *Windows 2000*-specific by checking the OS version. NTFS streams are virtually hidden from the users because *NT* commands and standard *Windows 2000* applications do not display them. Any given file on an NTFS volume is basically the first, unnamed stream of a file. Any file (or even directory) can have associated, named streams. These streams can be accessed via standard file operations. Most *Windows NT/2000* applications do not use named streams. Some applications, including the *Windows 2000* shell, use streams to write file property information into a named stream of a particular file. This way, additional information can be kept together with a file object without changing the actual file content.

The W2K/Stream virus is 3,628 bytes long. The virus is compressed with *Petite*, a popular Portable Executable (PE) file compressor. The virus code inside is very short but the actual, compiled standalone file would be at least 4 KB. First the virus checks the *Windows* version of the current system. If it is not *Windows 2000* the virus displays a message box.

This is basically a new sub-class of companion virus, a stream-companion virus. When the virus infects a file it replaces the host application with itself. Basically, Stream implements the simplest possible virus infection by overwriting the host program with its own code. In other words, each infected file will be 3,628 bytes long after the infection. The trick is that Stream saves the original host application as a named stream of the host program.

For instance, when NOTEPAD.EXE gets infected, the size of the file will change to 3,628 bytes. At the same time the virus creates a 'NOTEPAD.EXE:STR' stream that will have the copy of 'NOTEPAD.EXE' content. This way, the virus can execute the host program as long as the infected file remains on an NTFS partition. (The virus uses temporary files during infections and execution of the host programs. The 'STR' stream of the host is not executed directly.)

When someone copies an infected file to a diskette, the host program will be lost, since the diskette uses FAT instead of NTFS storage format. However, the virus and the host will be copied over the network from an NTFS to an NTFS partition with a copy command. W2K/Stream is clearly a 'proof of concept' virus. Whenever the STR stream is missing the virus will display its introduction message box.

The virus uses the file compression flag as an infection marker. It sets this special NTFS file attribute via the DeviceIoControl() API. This way, the used disk space of the virus is not that obvious, although the free disk space does not calculate with the actual size of streams on the disk. The virus will infect all files in the current directory that have an .EXE extension. It does not pay attention to the actual file type.

Neither does it mind the read-only attribute. During infection operations the virus uses temporary files to copy the data streams. As self-recognition is performed via the compression flag, the already cleaned applications will not get the infection again since the AV software will not remove the compression flag. The virus will obviously re-infect itself without a host. Therefore, the actual host stream might hold virus code only. Stream passes the command-line parameters to the executed temporary file that it creates from the STR stream.

We might see special reincarnations of the DIR-II virus idea for NTFS. It is very likely that new viruses and Trojans will take advantage of the NTFS streams in various ways. The support for on-demand NTFS stream scanning is trivial and repair will be important against future trends.

W2K/Stream

Alias:	W32/Stream, WNT/Stream.
Type:	Direct action stream-companion.
Payload:	Displays message box when executed on a non-*Windows 2000* system or if 'STR' stream is missing from the file.

Self-recognition in files:
Set the NTFS compression flag for the infected file.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

VIRUS CASE STUDY

A Portrait of Jini

Dr Igor Muttik
AVERT, Europe

The virus called X97M/Jini.a was first discovered in February 2000. When run, it drops an SHN.XLS file in the XLSTART folder. Despite being considered an intended, for a while all major AV scanners were able to detect and clean the virus shortly after it was first found. In such a situation, any outbreak is unlikely and we would normally only receive samples from users who have not updated scanning engines and DATs.

However, on 10 August our *AVERT* research unit in the UK received an XLS sample by email. The sample was from a customer – a big UK superstore chain – who claimed that an XLS was demonstrating unusual, virus-like behaviour. Still, neither our scanner nor any of our internal tools could find anything suspicious and even VBA heuristics were silent. The user, however, reported that the file triggered a macro protection message box in *Excel* and that once the spreadsheet was loaded a 'funny' SHN.XLS file had appeared in the XLSTART folder. This prompted me to take a closer look.

Initially, we thought the sample contained an unusual, nonviable corruption of the X97M/Jini.a virus. It took a great deal of time to establish that this is really a new virus and that it does replicate recursively. And it was great timing – within a week we received similar virus samples from two other companies, one of them heavily relying on *Excel* spreadsheets in their business.

But what is this new virus? Why did our tools let us down? The research carried out within *AVERT* revealed that we were dealing with a unique, viable corruption of the known X97M/Jini.a virus that was missing parts normally present in any VBA project (i.e. present in any VBA files with macros – be they .XLS, .DOC or .PPT).

Normal files with VBA macros have three components in the VBA project: compressed VBA source, compiled p-code for each VBA module, and executable codes (execodes) for all VBA modules. However, *Office* applications (and *Excel* is no exception) have the ability to use one of these three components if another is missing, corrupt or unrecognizable (e.g. created by another version of *Excel*).

That is what had happened – the mother X97M/Jini.a virus lost both compressed sources and p-code but had ready-to-use execodes. The new virus was later given the name X97M/Jini.a1 to denote its relation to the parent virus. X97M/Jini.a1 is a crippled but viable form of X97M/Jini.a and its VBA_PROJECT has only VBA execodes in so-called _SRP_n streams (n=0,1,2,3 etc).

When X97M/Jini.a1 replicates it is unable to return to its X97M/Jini.a state. And because VBA execodes are *Excel*-version specific the virus can replicate only under *Excel 97*. Other *Excel* versions would not understand the execodes and would not run the virus.

X97M/Jini.a1 got lucky – not one scanner used execodes to detect VBA viruses because compressed sources and p-code were easier targets. There was never any reason to scan execodes! Fortunately, our latest scanning engines have so-called ActiveDAT technology which makes it possible to implement in the DATs algorithms of any complexity. So, in a couple of days the problem was solved – scanning and cleaning of VBA execodes were implemented.

Now we knew how to solve the customer's problem and an EXTRA.DAT to detect and clean the X97M/Jini.a1 virus was sent to all the users who had the virus. The detection was also included in the regular, weekly DATs. The whole exercise took about 10 days (!) while usually the reply (and an EXTRA.DAT) for any new virus goes back in several hours. The X97M/Jini.a1 virus was described and announced to other AV experts on 22 August 2000.

At that point we encountered an unexpected problem. Some AV researchers could not replicate the new form of the virus and were arguing against the very existence of it. As time passed the mistake was, of course, rectified (subsequently, many confirmations of X97M/Jini.a1 virality were received from both AV researchers and from the field) and it was recognized that X97M/Jini.a and X97M/Jini.a1 are two different, viable forms of the same virus.

We still do not know how and where the very first sample of X97M/Jini.a1 was created. It could have been the result of incomplete cleaning by some AV product, the sample could have been manually handcrafted, or it could have been the result of experiments with a live virus. In any case, it caused a lot of trouble for both users and AV developers. We received yet another confirmation that playing with viruses is not a good idea. X97M/Jini.a1 is currently the only known case of a virus consisting of only VBA execodes. It carries the text:

```
'Hye. You have just got me.
It's shani a little jini. You may call me a
virus in your termenology
It's a good idea taking backup of you files.
I am freindly but get wild sometimes'
```

Please, in future let us be cautious, because if we do not many more viruses will 'get wild sometimes'!

And I would like to thank our customers – if it were not for their vigilance, this particular virus would have been discovered much later and could have caused a great deal more trouble.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

EDITOR 1989–1993

Edward Wilding

Maxima Group Plc, UK

In the early days there was something of a ‘gang mentality’ amongst the regular writers and contributors to *VB* – this was a time when the anti-virus industry frequently misbehaved by issuing grossly inflated claims and hype. *VB* took a resolute stance in dismissing the industry’s wildest players and revelled in debunking self-serving claims.

In retrospect, the early *VB* bordered perhaps on arrogance. I do not regret this – there really were some charlatans around at the time and snake oil was abundant. I maintain that with any good product evaluation, the results are *verifiable* and *repeatable* and, over the years, *VB* has set a fine tradition in differentiating the quality products from the ‘also-rans’.

The anti-virus software industry has certainly calmed down – the modern *VB* is a sea of tranquillity compared with the fisticuffs and black-eyes of yesteryear. The current harmony reflects a mature industry where the key players, having proved their endurance and commitment to the cause, have learned that peaceful co-existence is mutually beneficial.

The first edition of *VB* appeared in July 1989, bearing the distinctive *VB* logo on the masthead – red for infection, green for sterilisation. The edition contained short descriptions and hexadecimal search patterns for all known computer viruses – this comprised eight PC viruses (yes, eight) and a handful of Macintosh strains. The hex search patterns, a key feature of the early bulletins, retain a strong nostalgic grip – their recent demise is much lamented by certain veterans.

An unresolved debate at the time concerned the patterns and their copyright; was it vested with the virus writer, the researcher who extracted the pattern, or the publisher? To complicate matters further, it was also evident that software manufacturers were incorporating *VB* search strings within their products. Initially this caused me some irritation on the grounds that it was a possible copyright infringement.

Joe Hirst, *VB’s* first Technical Editor, correctly pointed out that the strings were selected and published *specifically* for the purpose of detection and that an attempt to deny this opportunity to commercial software houses would defeat the object of the exercise. *VB* never formalised a policy in this respect, stating merely that an acknowledgement would be appreciated should any software manufacturer incorporate the strings in its product.

Joe was a keen enthusiast of virus-specific detection and disinfection methods, as opposed to generic techniques. His prediction, that virus-specific signature and profile scanners would endure and ultimately dominate the anti-virus software market, has proved completely accurate, although maintaining and upgrading such devices is highly labour-intensive, as the principal software houses will testify.

Another concern was profanity, particularly with regard to sexual swear-words. It soon transpired that many (most?) virus writers were semi-literate and as is sometimes the case with such people, their ramblings can be extremely unsightly when deposited on the page. In the end, I decided that expletives should be reported verbatim. I drew the line, however, at one hoax ‘mainframe virus’; its EBCDIC detection string made the folks at *IBM* blush to their roots!

The first edition had one subscriber – a gentleman, I seem to remember, from *Sun Alliance Insurance*. A frenetic weekend in high summer was devoted to typesetting the bulletin using *PageMaker* and editing late submissions.

Most copy was forwarded on diskette as electronic mail was still in its infancy. Little did I know that eventually *Virus Bulletin* would gain world-wide celebrity (or notoriety) and grace the shelves of thousands of corporate, government and academic libraries.

The business plan indicated that 100 paid-up subscribers would be sufficient to pay for my daily beer and sandwiches. This target was achieved by October 1989, partly as the result of the Datacrime (Columbus Day) virus scare. As a side note and to set the record straight, early *VB* marketing material hyped this non-existent threat mercilessly – I regretted this at the time and still do.

That said, however, I would remind readers that we were operating at the time in a highly sceptical environment. There had been no ‘Melissa’ or ‘LoveBug’ at this time and many people were unconvinced that virus propagation was possible. Peter Norton, no less, had declared computer viruses were a myth akin to the alligators said to inhabit the sewers of Manhattan. I received a handful of calls expressing similar sentiments.

A pivotal event in *VB’s* embryonic development was the AIDS Trojan horse of December 1989. Dr Joseph Popp, an American citizen, mailed 26,000 copies of his pernicious Aids Information Program to businesses, hospitals and

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

research institutes throughout Europe. This episode is well documented, not least by *VB* itself, and caused pandemonium as hundreds of computer users unwittingly unleashed the hidden encryption routine contained within the program. Jim Bates reverse-engineered the Trojan and produced an antidote within a matter of days, and the officers of Scotland Yard's Computer Crime Unit were instrumental in the eventual extradition of Popp to the UK.

Enduring friendships were forged during such events – Jim Bates, Noel Bonczoszek (formerly of the CCU) and I eventually migrated to computer forensic investigation and we remain in regular contact to this day. I note that another virus guru, Dr Fred Cohen, has also recently entered the forensic field – is this a trend? Popp did wonders for the journal's circulation, but his abiding legacy is the UK Computer Misuse Act of 1990, an adaptable and powerful piece of legislation that has played a significant role in my working life since leaving *Virus Bulletin.*

I should perhaps expand on the key role of *VB's* technical editor. Fridrik Skulason assumed this role for nearly the entire period that I was Editor and did an excellent job. Fridrik forgave my persistent nagging – key questions, always, were 'what does this mean?' or 'why is this relevant?'. Programmers sometimes assume too much technical knowledge on the part of the readership (and sometimes from the Editor also), or occasionally become fixated on irrelevant points of academic interest only. Fridrik would explain, tirelessly and with commendable patience, why a new technical development was significant in language that I, a non-programmer, could understand. Dr Keith Jackson, who performed most of the product evaluations at this time, David Ferbrache, who acted as *VB's* Macintosh guru, and Jim Bates, who provided detailed commentary on viral characteristics, were equally lucid.

From a technical viewpoint, a couple of viruses struck me as particularly memorable. I recall a specimen called 1260 that caused momentary alarm when it was realised that no static detection string could be isolated within its code. Dr Alan Solomon coined the term 'polymorphic' to describe this class of virus, which, overnight, rendered my beloved detection strings obsolete.

Then there was the Whale virus. This was a convoluted, mountainous pile of excrement and blubber that deployed cunning defensive measures to prevent code analysis. This 'armour' caused excitement within the research community, despite the fact that this so-called 'virus' was about as charismatic as a bucket of stale porridge. To my limited comprehension its main defensive measures appeared to be twofold: one, it was too lethargic to infect anything, and two, many researchers who tried to analyse it died of boredom. For the record, Dr Peter Lammer harpooned the Whale by isolating a series of reliable detection strings.

Whale, like so many viruses, was strictly a laboratory curiosity. Realising this distinction, we introduced a prevalence table that itemised computer viruses that were contagious and 'in the wild'. This was an early and primitive example of computer virus epidemiology. I was gratified to learn that *IBM* were engaged in similar studies, albeit far more extensive and based on a far greater data set.

Dr Steve White revealed the results of his team's researches at the first *Virus Bulletin Conference* in 1990 – boot sector viruses were prolific throughout this period, notably Form and Michelangelo. Certain viruses became extinct due to technical progress. Brain, for instance, infected 5.25-inch diskettes – try finding a computer that can read one of those nowadays!

There was a lot of ground-breaking terminology at this time, with many now well-established descriptions and phrases being coined on the spot and appearing for the first time in the pages of *VB*. The emerging lexicon encompassed parasitic viruses, stealth viruses, armoured viruses, polymorphic viruses, companion viruses, overwriting viruses, boot sector viruses and multi-partite viruses. Paradoxically, however, I do not recall a single person ever mentioning the words *macro* and *virus* in the same breath!

On a day in 1992 or thereabouts, a meeting took place at New Scotland Yard. Around the table were seated most, but not quite all, of the prominent players in computer virus research and anti-virus software development in the UK. This was a remarkable achievement by the police, as it was no secret that, at this time, there was little love, affection or mutual understanding within the industry.

The police were proactive – I participated in the first search warrants and arrests for virus dissemination in the UK. The members of the ARCV team that had distributed a virus writing kit were simultaneously arrested during raids in various cities. Thus it was that I came face to face with my first ever virus writer – a sullen teenage boy (what else!) who had honed his skills from Ralf Burger's notorious textbook on virus propagation. We found the book, but the computer had vanished the previous week, hurriedly despatched to *Olivetti* for low-level formatting.

The police were to have more successes, most notably the arrest and successful prosecution of Christopher Pile, the first virus writer to receive a custodial sentence in the United Kingdom.

Undoubtedly, *VB* has raised standards in the industry and served as a useful sounding board for the research community. The fact that software manufacturers know that they can meet the strictures of *VB's* evaluation criteria and sustain that performance is reassuring to the industry and its customers alike. *VB* is also a voice of reason in a 'sound-bite', media-driven age.

In the distant past there were various attempts to launch rival publications. These usually exceeded *VB* on word-count, but this verbiage was frankly unappetising. In the final test, *VB* outlasted them all and now reigns unrivalled, both as a publication and as a conference. Happy Birthday, *Virus Bulletin*, and many happy returns!

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

ADVISORY BOARD 1990

Ray Glath

PCsupport.com, USA

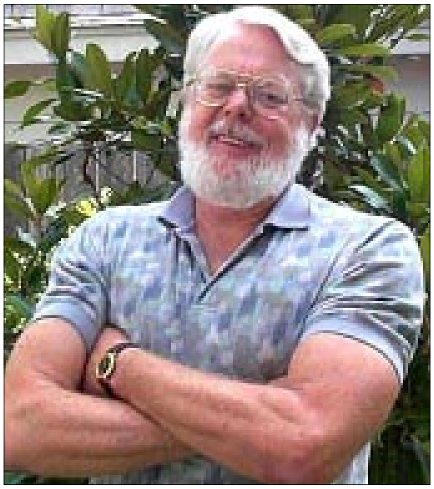
Everyone in the anti-virus field continues to operate in firefighting mode. No sooner is one fire extinguished, than another flares up. With the number of virus fires steadily increasing and the supply of fuel growing with each new PC purchase and each new Internet address, the problem continues to intensify. If you ask why PCs are still getting infected, you won't hear: 'We're using 10 year-old technology as our primary weapon.' You'll hear: 'The user didn't update his/her anti-virus software.' People have become conditioned to believe that the only way to fight viruses is with a scanner that needs constant updating. Something is very wrong with this picture. Does it make sense that we still rely on scanners to protect us from viral attacks when scanners need to be taught to identify each and every new virus that appears or they're useless against that new virus?

Are we living in the Twilight Zone when we see marketing claims (taken from the Web sites of major AV vendors this August) of '100% Virus Detection and Cleaning' or 'Clean files pass right through, but infected files are stopped before they can cause harm…Provides the best protection available, catching everything that looks remotely like a virus' – and yet witness massive epidemics caused by Melissa and Loveletter?

Over the course of ten years, one would think that the developers of virus-targeted platforms (e.g. *Microsoft*) and the developers of AV products would have banded together to create software to stop completely each class of virus once its infection techniques were learned. After all, these companies are filled with brilliant engineers. Surely they can out-think the Script Kiddies? And surely these companies can form better working relationships?

We saw that Melissa (and its variants) utilized the address book as a vector to spread itself. If a solid defence mechanism for this type of action was developed and deployed rather than simply adding 'definitions' for each and every variant, then the epidemic caused by LoveLetter and its variants could have been prevented. The first step is to change our mentality of having one AV scanning product for protection. Customers need to demand more from their vendors, *including* Microsoft. If different types of viruses utilize different techniques, vectors, and targets, then it's only logical that a multi-point defence perimeter is needed.

Next, our exposure should be only to those viruses which utilize new infecting techniques or those that infect new platforms. And, that exposure should only exist for a very short period of time until a new defence can be developed and distributed. Last of all, something different must be done. Looking back to Spring 1988 when I wrote my first paper on viruses, 'Computer Viruses, a Rational View', I find it interesting that the majority of advice I dispensed back then still holds true, even though it has been repeated ad infinitum by every emerging 'virus expert' and seems so rudimentary.



Back then, many of us had to exert substantial efforts to convince people that viruses actually existed. Those years were lean for AV companies. It took a while for us to realize that users had no interest in *protecting* themselves from a 'non-existent, unseen' threat. The products of that era were aimed squarely at *preventing* virus infections, primarily via 'behaviour blocking' and 'change detection' techniques exemplified by Ross Greenberg's *FluShot*; my *Disk Watcher*; Peter Tippet's *Vaccine*; and John McAfee's *C4*.

Once individuals were hit by a virus, they became believers in a hurry. But even then, they were only concerned with getting rid of the virus – it's a lot easier to take a pill after you get sick than it is to get a vaccination shot to keep from becoming ill in the first place. Thus, by the time of the first *VB* conference, the only technology acceptable to the public was scanning for viruses. The rest, as they say, is history. Marketing by the AV companies has been so effective that the term 'scanning' has become synonymous with 'anti-virus'. And once people finally did become interested in *protecting themselves* from viruses, the industry simply took the scanning model and wrapped it with a real-time component to scan files as they entered a PC.

So here we are. Still using the same old technology and living with the same old results, only today's epidemics are more widespread than anyone could have ever imagined. What can be done? Users must demand more from their vendors, and those of us in the AV industry must demand more from ourselves. Would the solution need to be one single program with 100% effectiveness? Of course not! When *you* get sick, there is no single 'super-aspirin' that will cure each and every ailment you may ever encounter today and tomorrow. We use different medications and treatment regimens for different maladies. The anti-virus medicine cabinet desperately needs improvement. There is a better way and we all must strive to find it.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

EDITOR 1993–1995

Richard Ford

Cenetec, USA

It's hard to imagine that over ten years have gone by since the very first edition of *Virus Bulletin*…, which means that it is eight years since my first association with the company. Time has flown by, and I had no idea then where the last eight years would take me. I must admit that I have picked up some precious memories on the way. I hope that you will indulge me, but before thinking about the state of the virus industry, I can't help but spend a moment reliving some of those times.

My first recollection of *Virus Bulletin* was day one as a full-time employee: Ed Wilding, the then-Editor, picked me up in central Oxford, and drove me to the airport. We were off to VB'92 in Edinburgh. After this baptism of fire, everything else seemed easy!

The next indelible memory I have of *VB* was Ed's last day at work – driving him home around the Oxford Ring Road, and realizing just how much work he had done in setting up *VB*, and the size of the task at hand. I was sad to see him leave, excited to be in control, and afraid of producing my first edition at the helm… all at once. I think I can still taste the crispness of the air that day; how vivid that day and the feelings still are.

Once fully installed as Editor in January 1993, the next few months passed in a blur. Each month appeared hot on the heels of the previous one, and I was always behind, trying to catch up. I loved it!

Months turned into years; next came the *VB* conference in Jersey, where I was to meet my future wife, Sarah Gordon. Nobody else knew it, but I think it was that meeting which ultimately drew me away from *VB*: the primary motive for resigning and moving to America was to be closer to Sarah, and make her my wife – a goal I finally accomplished on 4 December 1995, a year later. Almost five years since that day, we're still happily married and going strong… thank you *Virus Bulletin*!

While it's just plain good to riffle through these dusty but cherished memories, a lot has happened in the virus world in the last ten years, though in summary everything has been 'the same, but different'. That is to say, there is still exactly the same virus problem, solved mostly by exactly the same solutions, except the platform and its capability have been extended.

Sadly, I think we're in a much worse place than we were ten years ago: ubiquitous connectivity and automated email access have allowed viruses to spread with incredible speed. I personally believe that there is some sort of self-limiting effect – as the virus problem reaches a certain threshold, we, the users, start to take steps to reduce the problem. Below this threshold, we get careless, allowing more infections. Thus, in my opinion, we're in some sort of equilibrium – the impact of the problem is held within certain bounds that we ourselves set. My concern with this approach is that new virus attacks like Melissa can break out of this steady state and reach global prevalence more quickly than we can change our habits.

We continue to build applications that allow (almost beg for) exploitation by virus writers, and do not take preventative action until after it's too late. With omnipresent connectivity, I fear that the nightmare of a huge virus outbreak, with a significant portion of the world's computers unable to communicate with each other, is possible.

Sooner or later, the scenario I've described above will happen, it is only a matter of time and luck. Had Melissa been written differently, containing a suitably clever trigger routine, it could easily have been 'The One'. Fortunately, we got lucky… if we insist on running the ragged edge we won't be lucky every time. I hope I am wrong, but if I am, it will only be by chance.

It is tempting to try to blame the application vendors, but it is our fault as much as anyone else's. The anti-virus industry has not concentrated on developing technologies which can stop a meltdown occurring, and we, the purchasers of software, have voted with our software dollars *consistently* to reward functionality, not security.

While I have painted a somewhat dreary picture of the virus world at this time, I do feel that we'd be far poorer without *Virus Bulletin* – speaking for myself, both personally and from a corporate point of view. I met my wife through *VB*, and have a host of happy memories.

I also see a more aware group of users/developers, those who make good use of *VB* to keep up in this ever-shifting field. Thanks *Virus Bulletin*, and Happy Anniversary!

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

EDITOR 1995–1997

Ian Whalley

IBM TJ Watson Research Centre, USA

March and April 1995 were eventful months for me. Barely six months out of university (Manchester, one of at least three Universities worldwide with a reasonable claim to the title ‘birthplace of computing’), I found myself at the helm of *Virus Bulletin*, the longest-lived and most-respected journal of the anti-virus industry. I was not yet 22.

‘How on earth did this happen?’, I found myself wondering. And ‘how on earth did I *allow* this to happen?’ I found myself wondering months later. However, with the assistance of the redoutable Megan Skinner, the changeover from Dicky Ford to myself wasn’t too painful, and life soon returned to what passes for ‘normal’ chez *VB*.

Think back to early 1995. My desktop machine was a 486/66 running *Windows for Workgroups 3.11*. I forget the amount of memory it had, but it was either 8 or 16 MB (as I recall it seemed about as responsive as my current laptop, a PIII/700 with 256 MB RAM running *Windows 2000*). But what of the virus field? April’s *VB* contained analyses of Angelina (a boot sector virus – remember them? They were a problem once). It also featured RMNS and Nightfall (DOS file-infecting viruses – remember them? They were a problem once). It had an article about *FastDisk*, the protected-mode Int 13h replacement in *Windows 3.1* and later (remember *Windows 3.1*? It was a problem once), and a review of the *S&S Anti-Virus Toolkit* (remember *S&S*? It was …never mind).

I remember thinking, in late spring and early summer, that the sport of anti-virus didn’t appear to have changed very much in the last few years (I had been brushing up on my industry history). More and more viruses, ever-more complex iterations of the same old techniques (polymorphism, stealth, etc). In my optimistic moments, it seemed that the anti-virus was at least keeping up with the virus writers. Then, as has happened before and since, everything changed. August showed the arrival of Concept (see *VB*, September 1995, pp.8–9). Although it took a long time for the extent of the change to become clear, the arrival of Concept was remarkably well-timed for the *VB* conference.

Roll forward two years, to March 1997. That month, *VB* published my last comparative review as Editor. It featured 13 *NetWare* products – one of the harder breeds of product to review, although not the most time-consuming (anyone who remembers doing a DOS Comparative in the heyday of boot-sector viruses is not likely to forget the experience – just shy of 90 diskettes and over 20 products makes for a considerable number of diskette changes!). For this test, the most recently available WildList was October 1996, which contained a mere 13 *Word* macro viruses and one *Excel* macro virus. In spite of the fact that over a year had elapsed, the world of malware was still on the cusp of the true takeover of the macro virus – old-style DOS viruses still ruled the WildList.

September 2000 – as I write this, the world of malware is at another inflexion point. The latest WildList (August 2000) contained a comparatively small number of network-aware viruses/worms – a comparatively small number. But ask any member of the public to name two viruses, the chances are high that they will mention the LoveBug (aka LoveLetter), and Melissa.

The inflexion point at which we now find ourselves is the start of the true domination of the next big thing in malware – the age of the worms (doesn’t that sound like a 1950s’ B-movie? ‘GASP at the slime!’). The inevitable arrival of Internet-aware viruses (or whatever you want to call them) has been painfully obvious for several years – the far-sighted in the AV industry have been predicting it for longer than I’ve been in the business.

The new era of the Internet places ‘always on’ Internet technology in the hands of Joe Shmoe, the man on the street. Alas, Joe cannot afford a firewall, let alone a firewall administrator. Joe’s *Windows* machine cannot be secured – Joe could run a personal firewall, but the chances are high that he doesn’t, and running a firewall on *Windows* is akin to building a blancmange prison. Couple this with the general tendency of the computer-using population to click wildly on anything in sight and what do you have? The type of scenario that keeps people like me awake at night. I haven’t even mentioned the upcoming wireless Internet era – Internet to your phone, Internet to your PDA, Internet to your car.

But it’s not all doom and gloom. Modern anti-virus products have improved radically in the area of stability, functionality, and just plain detection. However, the ability of anti-virus vendors to keep up with the pace of events is still questioned – and rightly so. The standard of quality assurance and software engineering in the anti-virus industry is almost uniformly poor – the necessity for rapid responses to developing situations almost certainly contributes greatly to shortcuts in the quality department.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

ADVISORY BOARD 1997

Charles Renert

Symantec AntiVirus Research Center, USA

In 1994 when I began dissecting viruses for a living, the security battleground was a very different place from what it is today. Users were just beginning to take notice of viruses and the problems that they could cause. There were just over 1,000 viruses then, infecting primarily DOS executables, DOS boot records, and once in a great while, a *Windows 3.1* file (which generally didn't spread very far).

The viruses that spread the fastest were those that propagated via the notorious shared floppy disk. Viruses that were hardest to detect were those that used the trickiest techniques of the day to elude detection – memory stealth, encryption, and most painfully, polymorphism. Fortunately, threats rarely spread fast enough to cause widespread damage, and a monthly definition release was generally sufficient to keep things under control.

Today, almost all computers have some kind of AV protection for their data. There are approximately 50,000 viruses infecting a wide range of platforms, as well as Trojans, worms, backdoor programs, port scanners and password sniffers to detect. The growth of the Internet has enabled recent security threats to spread to millions of users in hours across networks and email. The need for a quicker response has increased the size of virus labs by a factor of ten. In short, things got ugly. The upside of this unpleasant turn of events is that it looks like the good guys are still managing to get by with the same model of bygone years: 1 – get sample, 2 – detect/repair sample, 3 – distribute cure.

This will not last, unfortunately. More disturbing than the sheer volume of threats is the *breadth* of the threat types that are coming to our labs these days. First, it is frequently much easier for the bad guys to create a new type of virus than it is for the good guys to develop the technology that can detect and cure it. If you need an example, you probably weren't around for the many months that it took anti-virus researchers properly to detect and repair the first macro viruses in 1995/1996.

Second, the growth of new infection targets continues to accelerate right in step with increases in computing power and available software. In future years, non-*Windows* platforms will continue to gain popularity (including the ubiquitous handheld devices), applications will pick up new macro capabilities, operating systems will be enhanced, and all of these areas will be ripe new areas for attack. Finally, security threats don't attack just files these days, or even single machines – they attack *entire networks*. File scanning, while still a necessary component of security technology, will not be sufficient to stop or clean future electronic nasties in all the new places that they will lurk.

Thus ends the doom and gloom portion of my discourse. I am of great hope that the most critical holes opened up by the continuing explosion of technology can be closed. Anti-virus researchers are going to need a few new tools though, and many of them are already in development. It is an easy prediction that firewalls, authentication and access controls will continue to expand, as the best line of defence against all threats is to prevent anything that is not known and trusted.

A middle layer will emerge that will also protect against unknown threats which I will call the *heuristic layer*. In addition to the classic AV heuristics of detecting certain classes of virus, this layer will also be able to monitor system and even network characteristics and classify certain sequences of events as threats and block them. If suspicious activity is logged that does not fit a known threat profile, it will be captured and sent off to the lab as 'needing further analysis'. Automated analysis machines and lab researchers (as necessary) will decide if the behaviour is a new kind of threat, a non-threat, or more information is needed; all responses (and cures, if necessary) will close the loop back on the user's machine. The final layer of technology will still be the good ol' scan for known threats. Also, system memory scanning will be developed and enhanced to detect and remove increasingly complex attacks properly.

I would have liked to say that advancements in security are moving in a proactive direction, but I do not believe that. My experience leads me to the conclusion that the most popular systems and software are rarely the most secure, and a great deal of effort in computer security will continue to be dedicated to reacting to new developments in these areas. It is not possible to predict with certainty which technological advances will emerge in the years to come, nor can one foresee the security breaches that they will introduce. This is not a bad thing – it's simply a reality with which any effective security approach must come to terms. So, regardless of what security model you employ today or in the future, I bring to you these words of caution: if you don't have an army behind you to adapt and secure you constantly against the changes that new technology brings, you've already lost the war.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

EDITOR 1997–1999

Nick FitzGerald

Computer Virus Consulting Ltd, New Zealand

‘What I did in my holidays’ – well, maybe not quite. Francesca has asked the former Editors to contribute something to add to the celebratory cheer of the tenth *Virus Bulletin* conference anniversary issue, and what the good doctor wants the good doctor usually gets (or so her husband told me!). So, what do I consider the most significant thing or greatest change I witnessed in my time as Editor at *Virus Bulletin*?

Considering the potential topics, I rejected ‘Francesca’s appointment as Assistant Editor’ as too sycophantic [*He’s definitely after something – what, I wonder? Ed.*]. I was left with much more mundane stuff from which to choose. After some reflection, I settled on the discovery of the true nature of the CIH virus.

CIH had already been isolated by a couple of anti-virus developers when it came to my attention. Richard Wang from *Sophos* asked if I had seen a cavity infector that cut itself into pieces then slotted those pieces into suitably sized cavities in a host. It then stitched itself back together from those pieces when the infected host ran. At that point, CIH was of interest for this novel infection procedure – apart from that it was just another *Windows 95* virus with a mindless, date-triggered, disk-trashing payload.

Richard accepted the task of writing a full analysis for the next issue of the magazine. Along the way, a small chunk of code in the virus’ payload resisted analysis. It was not armoured – we could see the code was manipulating ports and the like – but we could find no documentation of these particular ports in the usual reference materials. Resolved not to leave those few incomprehensible bytes of payload unmentioned in his first virus analysis to be published in *VB*, Richard eventually resorted to running the payload (on the analysis machine of another *Sophos* virus analyst who was away on vacation).

Perhaps fortunately (although not from that other virus analyst’s perspective), that machine had the right kind of Flash ROM to be affected by the now infamous BIOS-flashing part of CIH’s payload. Richard did not seem at all happy when this occurred late one afternoon, as I saw for myself when he called me to investigate the apparent death of the chosen sacrificial PC.

I have been told many times since, that what I saw that afternoon cannot be done. Believe me though, it is very eerie when a previously fine PC shows no signs of life, apart from the hard drives and fans spinning up, when power is applied – doubly so when you know the condition was caused by a simple program.

Anyway, Richard set out diligently to document what we had observed. Perhaps he was further motivated by concern at missing something the rest of the world’s top virus analysts were guaranteed to read with a close and critical eye. He uncovered technical specifications for *Intel* chipsets, programming sequences for various Flash ROMs and the like (killing the rest of the machines in the *Sophos* virus analysis lab was not an option – the lab manager was funny about that…).

Eventually, all the tech-specs tallied with the code in the virus and we were convinced that CIH was designed to reflash certain kinds of Flash ROMs, holding the BIOSes of their host PCs.

I do remember that telling the story of who should be concerned about this new threat was a whole other nightmare. It was made worse still, as even during investigation of the virus several reports of CIH moving quickly in the wild were confirmed from all round the globe, and the virus was soon appearing on magazine cover disks and the like.

Regardless of how the resulting coverage of CIH can be viewed, being directly involved as the full story unfolded and watching Richard’s detective work unfurl the first complete analysis of the virus was a great personal and professional pleasure.

Many other experiences stick in my memory. Being Editor of *Virus Bulletin* was not the primary reason I was targeted by the ColdApe virus, but it was responsible for the discovery that the *NT* version of a popular scanner could not detect boot viruses on diskettes containing no files.

I also vividly recall the behind-the-scenes wrangling over the RemoteExplorer virus, and the ensuing media debacle – with one developer blatantly attempting to sit on samples of this virus despite having made press releases predicting the end of civilization as we knew it.

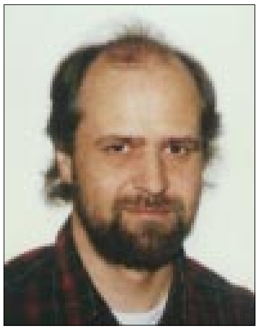
All in all, I enjoyed my time at *Virus Bulletin* and am thankful for the opportunities that arose there, and since, and for the new friends and strengthened relationships I developed during my time in Abingdon.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

ADVISORY BOARD 1998

Pavel Baudis

ALWIL Software, Czech Republic



I admit that I've never had the very first issue of the *Virus Bulletin* in my hands physically: the oldest issue in my bookshelf is 'only' from May 1990. However, the first issue is available in electronic format on the CD published from time to time by *Virus Bulletin* and it is quite interesting to look through it and find out what was the prevailing situation that time. And even though the appearance of the journal (and its price) has changed only slightly up to now, the problems being solved there differ substantially from those of today.

Ten years – is it many or few? In the field of IT it is sure to be a long period of time, during which plenty of things have changed radically. Naturally, there were far fewer computers then than there are today; there was practically no Internet; and communication among anti-virus specialists (but also among authors of the viruses) was difficult.

More importantly, in comparison with today, the spreading of viruses was very slow. Besides floppy disks, which at that time used to be the main distribution channel for virus spreading, there were only the BBSs (who remembers them today? As I've found out recently one such station has still been operated by us up to now but its activity has one big drawback – there are no calls to it at all and it's no wonder).

In those days, there was only one simple operating system for PCs: MS-DOS … Since then, plenty of things have changed. The situation concerning both viruses and operating systems, the state of applications and their mutual co-existence, Internet advancement and the massive usage of email is becoming much more complex and the events around us are happening much faster. Anti-virus programs cannot simply be written at home in one's garage – now it cannot be a one-man product anymore.

Formerly, we were kept waiting for the appearance of the next new virus for a relatively long time – even up to several months. Today, there are tens of new viruses appearing every day and their numbers are growing continuously. Boot viruses as well as classic file viruses are definitely in their decline but macro viruses and script viruses are advancing, exploiting new opportunities offered by poorly designed applications and especially email.

Unfortunately, the new and frequently dangerous properties of many of today's applications make this possible for them on a massive scale. Therefore, it is ever more important not only to identify the new danger but also to transfer its solution to the users as fast as possible in the most effective way. This must not be the sole responsibility of the anti-virus companies themselves any more, but also the result of an active approach from the users. Solving this task will be the biggest problem in the years to come.

For me personally, the last decade was an amazing period. Thanks to my work in the anti-virus business I have had the opportunity to visit plenty of interesting and exotic places, meet many interesting people and make many friends. What more could one wish for?

One thing has continually fascinated me in the development of anti-virus programs – namely, the technical co-operation of people from competing companies. Without this phenomenon one cannot imagine the functioning of the entire anti-virus business at all, and even despite this fact it is an entirely unique and unprecedented practice as far as other industries are concerned. In what other business sector could we find people in everyday contact, solving together new problems and discussing possible weaknesses and collaborating on improvements even in competing products?

At some stage all these contacts mostly have their climax at such events as the conferences organized by *Virus Bulletin*, where there is time enough to throw away the everyday problems and spend some time discussing things not necessarily associated with viruses, while drinking some beer sometimes all night long!

It is clear that *Virus Bulletin* has managed without any significant problems thus far and that it is well placed to respond to all the changes and novelties in the field of viruses and anti-virus in advance. Over the course of the years, *VB* has become an acknowledged, reliable, fixed star in the anti-virus firmament.

Also, the great conferences organized by *VB* belong in the absolute top category in the industry. During the entire period of its existence, the information in *Virus Bulletin* has been regarded as a very precious source and a constant inspiration for my future work. For many years to come, I sincerely wish to all those who work on and produce the journal and the conferences that their endeavour and vigour endures a long, long time.

P.S. Well, having said that, there's one very serious reservation I have in relation to the activity of *Virus Bulletin* over the last decade – despite several (very weak) attempts, none of the *Virus Bulletin* conferences has taken place in Prague! I hope that the *Virus Bulletin* staff will remedy this serious omission as soon as possible and that we can all meet again in Prague soon!

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

ADVISORY BOARD 1998

Sarah Gordon

WildList Organization International, USA

There are moments in one's life where the passing of time becomes incredibly apparent and, at least for me, anniversaries are such a time. It was therefore an incredible shock to realize that the upcoming conference in Orlando was in fact the tenth *Virus Bulletin* conference. Can ten years really have passed so quickly?

In order to commemorate such an event suitably, (and upon the irresistible coaxing of the current Editor), I have decided to share with you some of my thoughts about *Virus Bulletin*. While the technical content keeps me coming back, when I think about *VB* conferences, it is an image of Jan Hruska dancing in a tux, or Helen White and Marta Olafsdottir collecting balloons that springs to mind. As for the collection of photographs I've collected along with these memories… priceless! *VB* conferences are always a joy to attend, but for me, they didn't start out that way…

I still remember my first ever *Virus Bulletin* conference. Excited and nervous about presenting my work to a room full of anti-virus product vendors – work I was pretty sure they wouldn't especially appreciate because it went against everything they had been saying to the purchasing public – I arrived with some fear and trepidation.

Following a short 'lunch' (I had water) with Joe Wells and Dmitry Gryaznov I spent the entire rest of the first day alone in my room. Why? I was relatively unschooled in how conferences were organized. I didn't realise the cost of meals was included, so I didn't attend them. I was unemployed (just like I am as I now write this letter!) and I couldn't afford a cup of coffee, let alone a lavish dinner.

I wandered along the streets of Jersey alone the first night. Finally I found an apple – which I could afford – and that was my meal for the day. Back at the hotel, I wrote some letters, conditioned my hair, and went to bed – alone and terrified of facing all the famous AV people the next day.

The next day came. To my great relief, *Virus Bulletin's* Assistant Editor Megan Skinner, seeing my extreme discomfort and uncertainty, grabbed me by the arm and escorted me to lunch – assuring me it was paid for. I was very surprised when the then-Editor Richard Ford, whom I'd seen earlier in the day (but not met) seated himself across from me at that Megan-arranged luncheon – and even more surprised when he asked me for a tea break the next day! Wow! Those *VB* people were friendly after all!

That night, Alan Solomon (bless his heart) paid for my dinner. I could scarcely believe my eyes – sitting around the table were all of these famous anti-virus researchers and their wives, and there was me right smack dab in the middle of it. I was awestruck.

I guess I must have made a good impression – Alan asked me to do some work for *S&S Software* at Comdex (which I did); by the end of the conference I had been offered jobs by several anti-virus companies (I chose *Command* that time around); and, to top it all off, I was invited back to VB '95 in Boston! It was there, in fact, where my lunch companion of VB '94 (who had left *VB* and moved to America to pursue – so I thought – a job), and I made the formal announcement of our engagement.

Since then, I've attended *Virus Bulletin* conferences in Brighton, Munich, Vancouver … and now am antipcipating this one close to home, in Orlando. What have the past years brought? I've watched close friends come and go as Editors, Assistant Editors, technical gurus; I've watched the magazine go from a 'just viruses' publication to a much needed 'how viruses are part of the larger picture' publication. I've recommended users consult *VB* in every technical presentation I make. Computer magazines write about my work 'published by VB'; I refer journalists to *VB* for technical material on viruses. *VB* is part of my work-life, and that work-life is much richer for it.

To me, *VB* is much more than a source of techie material. It's a part of my own personal history now – and an important part. *VB* has undoubtedly affected the lives of many people with its focus on the computer virus problem – and that's really important. It was not only the first to publish scientific work on virus writers and the whole phenomenon of the virus writing subculture; it was first to discuss publicly the *Word* macro virus, the first to talk about the first *Excel* virus … the first to … pretty much the first on all major changes in the industry. More importantly to me, though, is the opportunity *VB* conferences have given to anti-virus professionals to interact with users. And, most importantly, *Virus Bulletin* made it possible for me to live happily ever after, by bringing me not only the opportunity to publish new research (which has made work a lot more fun!), but by introducing me to some of the nicest people God ever created. That's pretty much 'good stuff' for an organization to facilitate, and I'm ever-grateful.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

ADVISORY BOARD 1998

Shimon Gruper

Aladdin Knowledge Systems Ltd, Israel

It will probably be considered a cliché for me to say that the anti-virus industry has not changed significantly in the last ten years. Commercially available anti-virus products all still find the majority of the viruses using known signatures. Furthermore, anti-virus vendors still insist on signature updates and IT managers still struggle to distribute those updates to their users.

Hold on a minute though, there was a change. The anti-virus product signature updates are now provided on an almost daily basis and not monthly any more – that ensures more and more work for IT managers.

In spite of the fact that during the last few years many new threats have appeared, the anti-virus industry prefers to keep its head in the sand and solve those threats by adding their signatures to the already overloaded databases.

Let's face it, we all secretly know that there is *no* way that a signature-based anti-virus product will be able to stop the next LoveLetter-like outbreak by issuing yet another update. There is simply no way that this update could get to the user's machine fast enough to be there before the newly-infecting virus.

Meanwhile, the anti-virus vendors keep themselves busy competing against each other on how frequently they publish updates, completely ignoring the fact that their Web sites will simply crash should all their customers try to update at the same time (as it was during the LoveBug outbreak earlier this year).

Other people in this industry, for whom I have a lot of respect, spend time researching and developing worldwide network systems for an automated virus cure. When a new virus is found, a copy of it is sent to a central server that will automatically (or with manual intervention) analyse the new virus and send back a solution within a 'reasonable' amount of time.

I really cannot see how this system will work for the new Internet-malicious applications. It takes only a fraction of a second, after the infection, for emails with a copy of, say, LoveLetter to be sent to all the people in the address book. How can such a system cope with those fast-spreading beasts in a 'reasonable' amount of time?

It is about time that the anti-virus industry finally understands that in this Internet age we are playing a totally different ball game. It now takes only five hours for a new Internet-aware virus to become number one on the WildList, as opposed to the five years it took the Jerusalem virus back in 1987.

To be honest, I am not entirely sure that we can go on calling Internet-aware malware, for example LoveLetter and Melissa, viruses at all.

A virus, according to the accepted definition, must infect another file, but viruses like LoveLetter do not do that. On the other hand, they do use the Internet as their conduit and replicate through other Internet-enabled applications (WinSock, *Outlook* etc).

In spite of the fact that these malicious Internet applications are not strictly viruses, the anti-virus industry continues to label them as such, the press continues to write about the 'I Love You Virus' and users continue to believe that they will be totally protected if they have an anti-virus product on their machine.

I do not have a suggestion for a panacea, but it is absolutely clear to me that the anti-virus industry must stand up and say loudly and publicly that the traditional anti-virus scanner will *not* provide adequate protection against Internet-borne and Internet-aware malicious programs.

The real solution is a complex combination of security policy enforcement, user education and behaviour and new tools and technologies that must be developed.

The anti-virus industry should stop putting out fires with updates after the outbreaks have happened and think of some real *proactive* solutions. Those proactive solutions must provide real-time protection against unknown, potential threats mainly by enforcing security policies at the gateway or the desktop levels.

It is evident from the description above that such proactive protection should protect *in advance* – before a new malicious Internet program hits for the first time.

I am very well aware of the fact that many of the anti-virus vendors write 'Proactive' on their product boxes because they use heuristic analysis for malicious macros and scripts, but this is too little and too late and does not solve the real problem efficiently.

The bottom line here, and my tenth anniversary message as a member of the Advisory Board to the readers of *Virus Bulletin* and to anti-virus vendors is – 'Don't put out fires – prevent them instead!'.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

ADVISORY BOARD 1998

Dmitry Gryaznov

Network Associates Inc, USA

I remember how I was first introduced to *Virus Bulletin* not quite ten years ago in June 1992, after I had delivered one of my very first presentations at an international anti-virus conference. That particular event was the *NCSA's* annual conference in Washington D.C. *Virus Bulletin* then approached me, in the shape of Ed Wilding, the founding Editor of the magazine.

Ed suggested I make a presentation at that year's *VB* conference. He was kind enough to accept a paper that I might deliver even though it would be submitted past all the normal deadlines. Unfortunately, on my return from the States I managed to injure my foot and thus could not make it to the *VB* conference that year after all.

However, I caught up with the conference nicely the next year in Amsterdam in 1993. By that time I had participated in all the other existing international anti-virus conferences of that time.

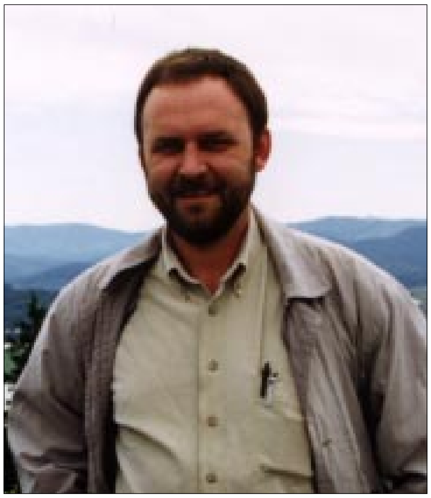
But the *Virus Bulletin* conference was (and still is!) head and shoulders above the others in all respects. Perfect organization, superb location, excellent presentations and outstanding entertainment – that, as I learned over the years, is a typical *Virus Bulletin* conference. Since then I have not missed a single VB conference and am looking forward to this year's.

And there is much more to *Virus Bulletin* than just the best anti-virus conference. Every time an issue of *VB* featuring a Comparative Review of anti-virus products' test results is due, anti-virus producers all over the world are literally holding their breath – so important and highly regarded have those tests become.

Add to this excellent articles on new viruses and other threats by the world's best experts and it becomes obvious why *Virus Bulletin* is rightfully considered the best anti-virus publication ever.

The anti-virus arena has changed drastically over the last ten years and past issues of *Virus Bulletin* are an excellent chronicle of this; from just a handful of viruses to hundreds to thousands to dozens of thousands; from rather simple DOS EXE, COM, boot sector and MBR infectors to complex polymorphics, stealth, tunnelling anti-heuristics viruses et cetera, et cetera …

And then, in early 1995, I came to think the game was mainly over – DOS was giving way to *Windows* and DOS viruses were doomed. But then the first *MS Word* macro virus appeared and it started all over again. When everyone had finally got used to macro viruses, Melissa came to play to demonstrate how effective and deadly a mass-mailing virus can be. It was soon followed by script viruses of which LoveLetter became the most well-known.



Meanwhile, the virus writers were building up the necessary experience in *Windows* programming, and now viruses for *Windows 9x* and *NT* are definitely gaining more momentum.

What is more, while in the not-so-distant past Trojans were not considered a serious threat when compared to viruses, today RATs (Remote Access Trojans) leaving PCs wide open and making DDoS (Distributed Denial of Service) attacks a grim reality, are probably no less a threat than viruses are.

If, several years ago, viruses spread from computer to computer mainly by means of magnetic media and thus the speed of their proliferation was mostly limited to that of trains and airplanes, today with just about every PC hooked to the Internet a virus can spread all over the world in a matter of hours if not minutes. And some of them do – like Melissa and LoveLetter.

With more and more applications and appliances these days becoming 'smarter and smarter', we are facing a new world where no file type and no digital appliance seems to be virus-safe. Documents, spreadsheets, presentations, even drawings can contain macro viruses.

We all saw Microsoft Word fall victim to malware and after that it was one after the other. *MS Excel*, *MS Access*, *MS PowerPoint*, *MS Project* all succumbed, and recently they have been followed by *Visio* and *AutoCAD*.

Apparently, Web browsing and reading email and news are no longer safe occupations either: HTML today more often than not carries this or that script code within it. Hand-held devices like *PalmPilot* can be infected too these days. Tomorrow it may be the turn of cellular phones…

Well, as in that ancient Chinese curse, we are living in interesting times. As interesting as at any time during the past ten years, I might add.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

ADVISORY BOARD 1998

Eugene Kaspersky

Kaspersky Lab, Russia

When I think back to the beginning of the 1990s, I definitely recall the Iron Curtain falling and my first trips out of Russia. My memory sweetly looks back to that sunny summer of 1992 when I had a pleasant day in Oxford and met the *Virus Bulletin* people for the first time. Sweet memories indeed!

Many things have changed since that time; much good and bad news have we heard; many anti-virus products have appeared and disappeared; the line of *Virus Bulletin* Editors is soon going to be longer than the list of Presidents of the United States – but even that doesn't deviate the journal from its path!

The Bulletin was, is, and seems to be continuing to follow the precedent of a highly professional and fast responsive journal where we can find almost any information about computer parasites and adequate protection against them (by the way, I'm still waiting for a 'Copsi-Cola' advertisement page somewhere in an upcoming issue, but it seems that will never happen).

The *Virus Bulletin* conference is a good opportunity for a new generation of anti-virus experts to present themselves, to start their public activity, as well as to get extra money for supporting their professional and personal needs (as I did for several years).

I can't predict precisely what will happen in the future, but I'm pretty sure that computer crime and cyber hooligans will not disappear (they will become older, and most of them will stop their virus/Trojan-writing activity, but new younger ones will enter the niches left in the line). I would say it's a feature of human nature and there is no chance of it ever being fixed.

Of course we *can* fix it but if that were to be the case, there would be no human race anymore. There will always be a part of humanity trying to self-actualize on the virus writing scene. The most frightening thing is that nowadays it seems to be becoming more prestigious to be a virus writer. Who knows, maybe in a few years we will see the setting up of special cyber-attack departments in defence ministries to make full use of this controversial human resource?

I don't think in the future it will be easier to catch virus writers and stop them annoying computer users. It is not the same as a case where you can simply 'disqualify' football fans who are being too aggressive just by moving them back to their homeland. Just imagine a hacker who is condemned to a three year 'out-of-keyboard' penalty. It's just not going to happen.

To my mind, the world's PC industry will never get rid of computer viruses and malware.

Unfortunately, quite the opposite is likely to be true – it is very probable that in the future viruses and Trojans will migrate to other platforms and environments, like, for example, hand-held devices.

When this happens (as it's bound to eventually) maybe we'll start to see multiple editions of *Virus Bulletin* being published: 'PC Virus Bulletin', 'Mobile Phone Virus Bulletin', 'Home Appliances Virus Bulletin', 'WC DDoS Attack Reports Virus Bulletin' … Who knows? [*World domination? I like it! Ed.*]

In my opinion, the main achievement of the anti-virus industry over the last ten years is that anti-virus protection has become an essential part of computer hygiene and day-to-day practice for anyone who owns and uses a computer. Certainly, for quite a long time I haven't seen a corporate network without any virus protection.

The most amazing thing is that nowadays even the average home user installs an anti-virus program. Together, the anti-virus companies have managed to convince the public that computer viruses pose a very real threat, and now I would estimate that at least 99% of the world's PCs are equipped with never-sleeping virus guards.

A couple of days ago I was sorting out my personal home library and for the first time (what an observant person I am, huh?) I noticed that *Virus Bulletin* hasn't changed a bit! It looks exactly the same as it did when the first issue came out ten years ago!

OK, to be fair I know it is more colourful and it has gained some more pages, the Letters Pages, the corporate comments etc. And seriously, I would like to say that it is still, after all these years, the most authoritative virus-related publication there is. *Virus Bulletin* delivers to customers all around the world not just some amateurish bluff, but comprehensive, professional, in-depth and trustworthy details on what is *really* happening in the virus world.

So I say, more *VB* – less VX. Happy birthday and long live *Virus Bulletin*!

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

ADVISORY BOARD 1999

Costin Raiu

GeCAD srl, Romania

Personal Log entry: 'Sunday, another dark, gloomy morning in New Cubeshire. Like fifty percent of the days of the year, actually. I watch the people passing by the small street where my home is located. Hudson 25 Street, not very far from The Hive, where my office is.

In the office, I see the September 2010 issue of *Virus Bulletin* on my desk, along with the associated X-DVD where the latest updates of anti-virus products, tools and all the other demos are located. The titles of this month look interesting; another miliary facility down because of the Guybr worm; the number of systems trojanized with the Dekox nail-mole reaches one million; the most reported virus this month – Jaix, of course. Usually, our cyber TS systems register over 100 reports each day.

I prepare a stim-tea and while the machine is making all those funny noises I hear each morning, I remember how *Virus Bulletin* was 10 years ago. Back then, if I remember correctly, the Internet was in full expansion and the direct effect of this was found in almost every successful worm written for the then dominant operating system – *Windows*.

But the years have passed, and they have brought surprises for everyone – for us, the anti-virus researchers, for the users, and for the operating system developers. What will happen ten years from now? That's probably as hard to say as it was for me ten years ago, when I was asked to write some words for *VB*. One thing is certain: software security will always have its place in our lives… September 2010, Costin Raiu, L2 Virus Cyberfighter.' Log end.

Returning to the present, I hope you enjoyed my short vision of the future. I couldn't help writing it because every issue of *Virus Bulletin* brings something new, something special to us all. For example, often when a new issue of *Virus Bulletin* arrives on my desk, I cannot avoid thinking how life would have been without it. Ten years of existence is a very long, long time.

Unfortunately I must admit that out of these ten, I can only cover three, since I was only introduced to *Virus Bulletin* in 1997. Maybe some of you remember the September 1993 edition of *VB*. This moment in time is a milestone, since it was the first issue to bring the look and style of 'Bull' we are still seeing today.

I also remember the first issue of *Virus Bulletin* – don't worry, I didn't read it ten years ago when it was first published, but only about two years ago, when I had the chance to get my hands on a CD containing electronic versions of all the old issues of *VB* ever since its birth.

If you missed it, I suggest you obtain one; it will give you a good view of what occurred in those ten years, trust me. If you also wonder what was in this first issue of *VB*, you're in luck. There was a Guest Editorial written by Dr Keith Jackson, who still wrote great technical product reviews until recently, and a contribution from the Technical Editor from back then – Joe Hirst. We also have the traditional list of known *IBM* PC Viruses, and the now-dead list of Mac viruses.

There is also an interesting Case Study as well as a Letter From Europe, then the classic, and still my favourite, Virus Analysis pages or 'Virus Dissection' as they were called back then. Pretty nice – in that issue we had the chance to see Jerusalem and Fu_Manchu stripped naked to their bits.

If you wonder what the first anti-virus product reviewed by *Virus Bulletin* was, you wouldn't be wrong guessing *Dr Solomon's AV Toolkit*. And last but by no means least, we should not forget about a Conference Report from Italy, and a list of upcoming IT-related events.

Comparing this first issue to the issues of the present, I haven't listed too many differences. Actually, I like this classic 'British' continuity in the magazine. It suits it quite well, and I certainly hope I will still see it ten years from now. I also appreciate that *Virus Bulletin* was the launching point of many new talented people, and it is still the place where you can see a masterpiece virus analysis written by one of the heavyweight old-timers.

However, contrary to the tone of my short futuristic story at the beginning of this piece, it is quite hard to imagine how the anti-virus world will look in ten years' time, and how *Virus Bulletin* will look by then. In the programme of the VB2000 international conference, I see scheduled a very interesting presentation which also deals with the issues of both the future and the past. I'll try not to miss it, and I'll also try not to miss the September 2010 issue, along with its enclosed small, shiny X-DVD…

PRODUCT REVIEW

SOFTWIN AntiVirus eXpert 2000 Desktop v5.7

Matt Ham

SOFTWIN's AntiVirus eXpert, or *AVX* for convenience, is a recent newcomer to the *VB* Comparative testing regime. While new to *VB's* prying eyes the product has, like its many fellow Eastern European comrades, a considerable history in its native land. Along with these other companies, *SOFTWIN* is attempting to spread its market further. *SOFTWIN* is unusual in this group, and to a lesser extent in the anti-virus market in general, since it performs a wide range of activities both in and outside Romania, including software outsourcing, document conversion, and electronic publishing services.

AVX starred in the July *VB Windows 98* Comparative, so the speed tests have been mostly omitted on this occasion as they were amply covered then and are only useful when applied in a relative fashion against competing products. For this standalone review the product was tested on an *NT* workstation, since any stability problems on a different platform, of which there were thankfully few, would definitely be relevant.

Considered below are the various scan modes offered by *SOFTWIN'S* detection machine and the ways in which this detection has been implemented. Some speed tests are considered, though they are relative to *AVX* itself. A customary rhetorical question at this point leads on to the main text – will all be well?

Packaging and Documentation

AVX was supplied in two different incarnations for the testing, relating to the disparate distribution methods inside and outside Romania. The version tested was a slightly more recent vintage of the application in electronic format, though the boxed version, available only in Romania, was also inspected. As was a past custom, now joyfully revived, the packaging, arriving in a crushed state from the courier, was subjected to a sturdiness test, which it failed. More distressingly, the electronic version first downloaded suffered the same fate, arriving in a corrupted form. Matters improved with a second attempt – the contents of the box proved to be intact, and the testing was ready to commence.

The contents of the box were not huge in number, consisting only of the CD in a cardboard wallet and a (relatively thick) manual. The latter appeared to be of good quality and detail, though as this reviewer's knowledge of Romanian is somewhat limited, any such theory is derived purely from appearances. With the electronic version of the package there came, as expected, PDF documentation in English, though not as an integral part of the product ZIP file. This document is, for an early release of the international version, a surprisingly good piece of documentation. Admittedly there are a number of minor grammatical oddities present, including the odd typo (unless *SOFTWIN* really does have access to '32-byte' systems), but the overall level of information and clarity was impressive. Some of the newer features of the *AVX* version for review were absent, which did, on the other hand, prove irritating.

Installation

The process of installation these days seems to vary little from product to product, though *AVX* managed at least to add some cosmetic pleasantries to the affair. The level of configuration, once past the standard licence and installation requirements, is very high if a custom type is selected. This allows the omission of most of the program options other than the core on-demand scanner.

It is a trifle worrying that the on-access scanner is considered an optional component, though elsewhere it is stated that this function is of paramount importance – but it is pleasing that the user is given so much choice.

Scanner Options

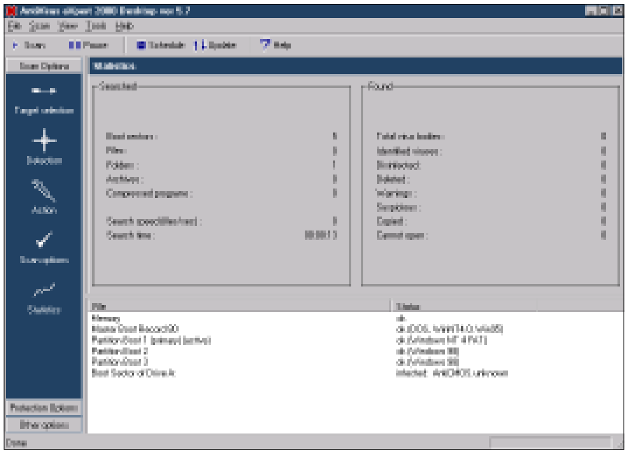
The interface of this product is pleasantly uncluttered and tends towards the functional rather than the decorative, though the icons used are reminiscent of some game lodged deep in the reviewer's subconscious. There is also a slight sense of disorganization to be felt when applying configuration options since, although there is a fine level of control, the commands for a particular function are often spread between several different locations.

There are the usual drop-down menus, these by and large duplicating the more easily navigable toolbar and main menu area while supplying a useful area for the saving and restoring of the overall application configuration. These saved configurations are unlimited in number.

Hidden away under the 'Help' part of this section is also one of the more interesting sources of information about the internals of the product. *AVX* uses a modular system, allowing for program updates to occur by the addition or alteration of small plug-ins rather than a complete engine replacement. This helps to explain the ease with which such options can be selected during installation. Here, in the 'Help' section, is stored a list of these plug-ins, each with a name sufficiently descriptive as to be easily related to a certain function.

Using this list, it is possible to determine that most of the present modules are related to archive scanning, the selection here being wide, with a variety of heuristic and

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.



Statistics

Searched

Boot sectors : 6
Files : 0
Folders : 1
Archives : 0
Compressed programs : 0

Search speed(files/sec) : 0
Search time : 00:00:13

Found

Total virus bodies : 0
Identified viruses : 0
Disinfected : 0
Deleted : 0
Warnings : 0
Suspicious : 0
Copied : 0
Cannot open : 0

File	Status
Memory	ok
Master Boot Record(0)	ok (DOS, WINNT4.0, Win95)
Partition Boot 1 (primary) (active)	ok (Windows NT 4 FAT)
Partition Boot 2	ok (Windows 98)
Partition Boot 3	ok (Windows 98)
Boot Sector of Drive A:	infected: AntiCMOS.unknown

general scanning modules making up the bulk of the remaining modules. With the detection modules, each notes the number of associated definitions, ranging from over 20,000 for the 'Code Emulator & Virus Analyser Plug-in', down to four for its equivalent 'Hlp Engine Plug-in'. Only one plug-in remained particularly mystifying – the 'AVX Optical Recognition Engine', which brings to mind all manner of impressive possibilities.

The toolbar is the home of a 'scan and pause' scan control, links to the scheduler and update trigger, and the now customary help resource. This last did not seem to be working, presumably a casualty of the ongoing internationalization of *AVX*.

The main control area can be toggled between settings controlling 'Scan Options', 'Protection Options' and 'Other Options'. The first is obvious; the second controls on-access scanning of 'Net downloads, mail, updates and the scheduler; and the third controls language, offers a link to the *AVX* virus information Web resource, allows log viewing and offers a link to the non-existent help file.

The Scan Options section is where the bulk of activity occurs, these options containing the usual selection of controls and tweaking capabilities. A further division can be made at this level, with Target Selection, Detection, Action, Statistics and again, Scan Options – each bringing up a different page of associated information. Targets may be selected at drive, folder or file level, with a browse option available and network drives included.

'Detection' is more complex in its controls, adding to the usual boot sector memory options to check email, verify Internet ports or check system security. 'Action' offers the usual features of ignore, prompt, disinfect, delete or quarantine, with a selectable quarantine file. 'Scan Options' is the area where 'warnings', of which more later, are enabled and where heuristics too are controlled.

Lastly in this section, the log file may be viewed, though oddly enough its configuration is spread among several of the aforementioned control areas. *AVX* errs on the side of caution in all areas except archives, activating heuristics, warnings and scanning of all files by default.

The Protection Options commands are a mixed bag indeed, with the scheduler looking a little out of place. *AVX* can be selected to perform scans of downloads and within mail, and there are alterable scan settings for these activities in this area. The download scanner autodetects common scanners when requested to do so, while the mail scanner seems more aware of mail applications, not requiring a manual search command.

As is traditionally found in schedulers, the time between scans can be set across the range from hopeful to ridiculous in terms of years and seconds respectively, though otherwise it is functional and easy to configure.

Other Options

The on-access component of *AVX* is slightly odd in that it operates almost totally divorced from the main program. All control over this aspect of protection is achieved through the right-clicking of the startbar icon, though there are few configuration options to choose from. Statistics can be viewed in real-time or sent to a log file – irritatingly, this defaults to the same log file as the on-demand scanner but this is easily changed.

The most irksome feature from the review point of view, however, is that *AVX* does not scan on simple file opens. Together with *Windows'* penchant for aborting copies when one file is refused access, this renders it impossible to test the on-access component in any realistic way.

The Tests

The standard scanning mode for *AVX* is to scan all files with heuristics enabled, which is sensible enough if there is enough raw throughput rate. Archives are not scanned by default, though with the *VB* test-sets this should make no difference unless the archived WildList is used. Nevertheless, each of these settings was varied in order to analyse the differences made by each.

As far as detection was concerned, the results of comparing the settings of heuristics 'off' or 'on', and 'program' or 'all files' were reasonably predictable. Dropping to 'programs only' rather than 'all files' resulted in the missing of 29 more samples. Removing heuristics resulted in a much bigger loss in detection, down 731 from the original score, while removing both 'all files' and heuristics lowered the detection by a total of 749 files.

Clearly, the heuristics in *AVX* are a valuable part of the program. As far as detection goes, the settings are at their best in default mode, which was therefore used for the calculation of the figures in the table overleaf.

SOFTWIN will have good reason to be pleased with these results, despite the obvious weaknesses in the Polymorphic and Standard sets. Most pundits would agree that the ItW viruses are the most important ones to be most ahead of, with macro viruses being the most prevalent source of new

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

On-demand tests	ITW File		ITW Boot		ITW Overall		Macro		Polymorphic		Standard	
	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%
SOFTWIN AVX	3	99.42	0	100	3	99.50	0	100	1011	89.40	92	95.43

entries into the WildList, though the latter claim is open to debate as more script-style worms appear. The Macro test-set was fully detected by *AVX*, and samples of JS/Unicle and W95/Babylonia posed the only problems on the WildList. This is a good result, especially when it is noted that the large number of standard misses was made up, by and large, by antiques or curios rather than those samples which have caused problems recently.

This leaves the Polymorphics as the great sticking point for *AVX*, with there being more to worry about in terms of detection. However, problems such as ACG are shared by several other well- regarded scanners.

The first great surprise came in the raw scanning rates. *Virus Bulletin* sets no great store by the scan rates over the test-sets since these are totally unrelated to real-world situations – thousands of different viruses are unlikely to appear on one machine. In this case, the times are worthy of note, however, by dint of being all but constant.

The first four scans performed were all within ten seconds of 58.5 minutes, a negligible difference over what is a comparatively long test time. The first thought at this point was that screen output was the limiting factor.

It is notable, especially under *Windows 98* where smooth scrolling is implemented, that scans are often limited by screen throughput rather than application speed, and during comparative testing it is usually the case that minimized scans are run.

A scan was therefore repeated in minimized mode to test this theory, with the minimized scan indeed showing a speeding up of the operation. For this reason the false positive/scan speed tests were performed with the application minimized. Here, the situation became less clear cut.

In the standard setting, with heuristics enabled, the Clean set gave 22 spurious warnings and one definite identification of Natas.4746 – a situation which tarnishes any set of detection results. The same Clean set scan was performed without heuristics enabled and this time affairs were marginally better. The time taken was decreased, though not to an epic extent, and all the warnings removed. To counter this, however, the false positive remained a blot on the *AVX* copybook.

Another area where improvements could be made in *AVX* is the matter of the scan start times. Although most of the review scans performed as expected, there were several occasions when the product became very sluggish at the beginning of a scan, sometimes taking several minutes during the scanning of memory and boot areas.

Other Features

In the description of the interface, passing reference was made to the update configuration area. The update system, perhaps controversially named ‘AVX Live!’, allows for automated updates to occur either via a local update repository or directly from the *SOFTWIN* servers. The system is not quite as subtle and ‘behind the scenes’ as some others, having a tendency to lurk on the startbar resplendant in its yellow and red plumage.

Conclusions

SOFTWIN, as mentioned before, is a company new to the English-speaking world, at least as far as anti-virus software is concerned. The product is, however, far more mature than this situation might suggest. *AVX’s* basic detection ability is clearly good in default mode, due in a large degree to the sensitive heuristics.

These heuristics are, on the other hand, the cause of some very irritating and potentially time-consuming false positives. With heuristics removed the detection rate drops to a much less reasonable level, and the user is placed to a certain extent between the devil and the deep blue sea when choosing whether to activate heuristics or not.

Apart from this niggle, relatively important as it is, the product has all the features to be expected of a workstation standard, though they are arranged more chaotically than might be desired. There is also a distinct lack of heavy-weight central administration tools which could be seen as a possible next step for *SOFTWIN*. However, *AVX* is under constant change – the review version itself is a new version due for release this month – and thus the hoary old adage of ‘this is one that we shall watch with interest’ remains truer than ever.

Technical Details

Product: *AntiVirus eXpert 2000 Desktop v5.7*.

Developer: *SOFTWIN SRL*, Str Fca de Glucoza 5, Sector 2, Bucharest 72322, Romania; Tel +40 12330780, fax +40 1233 0763, email sales@antivirusexpert.ro, WWW http://www.antivirusexpert.com.

Price: 1 user – US$35, 10 users – US$150, 100 users – US$900.

Test Environment: Workstations: Three 166 MHz Pentium-MMX workstations with 64 MB RAM, 4 GB hard disks, CD-ROM and 3.5-inch floppy, all running *Windows NT*. The workstations were rebuilt from image back-ups, and the test-sets were scanned on local hard drives or CD-ROM.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/Win98/200009/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

ADVISORY BOARD:

Pavel Baudis, Alwil Software, Czech Republic
Ray Glath, PCsupport.com, USA
Sarah Gordon, WildList Organization International, USA
Shimon Gruper, Aladdin Knowledge Systems Ltd, Israel
Dmitry Gryaznov, Network Associates, USA
Dr Jan Hruska, Sophos Plc, UK
Eugene Kaspersky, Kaspersky Lab, Russia
Jimmy Kuo, Network Associates, USA
Costin Raiu, GeCAD srl, Romania
Charles Renert, Symantec Corporation, USA
Roger Thompson, ICSA, USA
Fridrik Skulason, FRISK Software International, Iceland
Joseph Wells, Wells Research, USA
Dr Steve White, IBM Research, USA

SUBSCRIPTION RATES

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, The Pentagon, Abingdon Science Park,
Abingdon, Oxfordshire, OX14 3YP, England

Tel 01235 555139, International Tel +44 1235 555139
Fax 01235 531889, International Fax +44 1235 531889
Email: editorial@virusbtn.com
World Wide Web: http://www.virusbtn.com/

US subscriptions only:

VB, 50 Sth Audubon Road, Wakefield, MA 01880, USA

Tel (781) 2139066, Fax (781) 2139067

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 on each page.

END NOTES AND NEWS

The Black Hat Briefings will take place at the Radisson SAS hotel, Amsterdam, Holland from 24–25 October 2000. Topics scheduled to be covered at the event include hacking, DDoS attacks, defence against kernel modifications and all aspects of network security. There will also be hands-on training offered. For updates and to register contact the event organizer; Tel +1 916 853 8555 or visit the Web site http://www.blackhat.com/.

***Netconnect* is to host a workshop on 'Management of Internet Security'** from 31 October to 2 November 2000 in London. The course costs £1,195. For details contact Adelle Shedd; Tel +44 1223 423523 or email training@netconnect.co.uk.

CompSec 2000 takes place from 1–3 November 2000 at the Queen Elizabeth II Conference Centre in Westminster, London, UK. The 17th world conference on Computer Security, Audit and Control focuses on all aspects of e-commerce and IT security. For more details, visit the Web site http://www.elsevier.nl/locate/compsec2000 or contact Gill Heaton; Tel +44 1865 373625.

***Sophos* is to host a day-long course entitled 'Managing Internet Security' on 14 November 2000** at the organization's training suite in Abingdon, Oxfordshire, UK. From 15–16 November a two-day course on 'Implementing Windows NT Security' will take place at the same location. For more details about the different courses and training days available, or to reserve your place, contact Daniel Trotman; Tel +44 1235 559933, or email courses@sophos.com.

The Windows 2000 eNTerprise Exhibition and Conference is to be held in the Grand Hall at Olympia, in London's Earls Court from 21–23 November 2000. For further information about the event contact Deborah Holland; Tel +44 1256 384000.

AVAR2000, the 3rd annual conference of the Association of Anti-Virus Asia Researchers will take place from 28–29 November 2000 at the Shinagawa Prince Hotel in Tokyo, Japan. For more details email haru@jcsa.or.jp or visit http://www.aavar.org/.

The Internet Business Exhibition & Executive Conference takes place at the Brighton Metropole, UK from 5–6 December 2000. For more details contact Richard Cole; Tel +44 1273 773224 or visit the Web site http://www.ibshow.com/.

The 16th Annual Computer Security Applications Conference (ACSAC) will take place from 7–11 December 2000 in New Orleans, Louisiana, USA. Email publicity_chair@acsac.org or visit the Web site http://www.acsac.org/ for more information.

The UK Security Show 2001, incorporating The IT Security Showcase, is to take place in Hall 2 of the Wembley Arena in London, UK from 14–15 February 2001. The line-up includes interactive product demonstrations and practical installer workshops alongside study-based seminars and debates and more traditional conference-style presentations. For more details about the event visit the Web site http://www.securityshow.com/.

The organisers of **iSEC Asia 2001, to be held at the Singapore International Convention and Exhibition Centre from 25–27 April 2001**, are looking for companies wishing to exhibit at the event. The conference and exhibition covers IT security topics from anti-virus through encryption to biometrics and digital signatures. For more information and a booking form contact Stella Tan; Tel +65 322 2756 or email stella@aic-asia.com.

Symantec* has launched *Norton SystemWorks 2001, the first multi-platform edition of its utility suite with support for *Windows 9x*, *Windows Millennium*, *Windows NT* and *Windows 2000*. The standard edition is available now for an estimated retail price of £59.99 at *Symantec's* on-line store at http://www.SymantecStore.com/.

According to recent studies by *InformationWeek Research*, the cost of computer virus damage to global businesses will be approximately US$1.6 trillion this year alone. The research covered organizations across 30 nations and concluded that a loss to productivity as a result of computer downtime following a virus outbreak was the greatest threat to businesses worldwide.

The DonaldDick Trojan, first discovered in September 1999 and enjoying something of a revival, is being hyped by the media as bearing a malicious attachment under its subject line 'Erap Estrada' (the nickname of the President of the Philippines, its country of origin). The anti-virus industry has been quick to condemn the exposure given to this Trojan and assures users that regularly updated anti-virus software will have no problem with this latest effort.

VIRUS BULLETIN **©2000 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /2000/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.