CONFERENCE REPORT

VB 94: The Return to Jersey

The small island of Jersey, just off the French coast, was the setting for the fourth annual *Virus Bulletin* conference. This gave a sense of déjà-vu to many delegates and speakers: the *Hôtel de France* in St Helier hosted the first ever *VB* event, in 1991. Participation was up on last year, with over 200 people from near and distant shores representing both the technical and the corporate sides of the anti-virus world.

Conference Overview

Every year, particular themes tend to surface again and again. At *VB 94*, the first, and most often reiterated point, was that computers do not spread viruses; people do. Virtually every speaker pleaded for more user education and awareness - without these, it was argued, there can be little hope of winning the war against viruses.

During and after sessions, much discussion concentrated on the role users could or should play in attempting to discourage virus writers from continuing their pastime. Many industry luminaries said that it was time corporates sent a clear message of 'we don't like what you're doing'.

In the Beginning…

The Wednesday before the start of the conference proper saw an informative and enjoyable discourse on viruses in general, presented by Dr Jan Hruska of *Sophos Plc* and Dr Steve White of the *IBM TJ Watson Research Center*. This double act is rapidly becoming a conference institution, and provides an excellent way for delegates to catch up with the current state of play before the conference begins.

Thursday morning saw delegates creeping into the main auditorium for the opening address, still fuzzy from a Wednesday evening which ended in the 'wee small hours'. *VB* editor Richard Ford, however, soon woke everybody up with his factual and rather depressing assertions that viruses will continue to proliferate, and that virus source code will be more readily available - thanks in no small part to actions such as those of Mark Ludwig and his infamous CD-ROM. Ford's opening address set the tone for the conference: the past year has seen ever more complex virus code, and increasingly bold actions by both virus authors and distributors. 1995 looks likely to provide much more of the same.

Alan Solomon of *S&S International* then took centre stage, regaling the audience with his experiences with virus writers. Delegates learned about the *ARCV* (*Association of Really Cruel Viruses*) and the people behind it, and of Solomon's view that, though such people may exercise their freedom to write viruses, we as users should exercise exactly that same right to try to stop them.

Mechanics and Management

After Solomon's talk, the conference separated into technical and corporate streams. Kicking off the technical stream was Paul Ducklin, of the South African *CSIR* (*Council for Scientific and Industrial Research*). Ducklin, an energetic and entertaining speaker, firmly believes that in many ways the effort to educate made by both the corporates and media has missed its target. He cited the misunderstanding still surrounding viruses such as Stoned as an example of the problem. The virus can be detected and cleaned with standard DOS commands. Why, then, does it still cause so much trouble? His conclusion, reiterated many times over the next two days, was that users must become more aware, and that education must also be directed towards virus authors themselves. It is not enough just to have a well-informed technical support department.

The technical stream continued with a live (and lively!) demonstration of a Virus Exchange Bulletin Board in the USA, by Jeremy Gumbley of *Symbolic*, who accessed a VXBBS to show delegates how easy it is to obtain viruses. Such action is not possible in Italy, where Gumbley lives, as virus transmission is illegal. This is not the case in most of the rest of the world, and Gumbley posed the question of how best to address the issue. During the presentation, Gumbley left a tongue-in-cheek note to the board's SysOp. Interestingly, the account used has since been closed…

While these technical issues were being addressed, Edward Wilding, *VB's* founding editor, now turned hi-tech 'super-sleuth', was directing a presentation to the corporate stream, discussing how best to detect and prevent illegal computing activities. His ultimate recommendation was for the implementation of legal guidelines to assist those encountering the use of computers in criminal and civil cases.

The Big Blues Brothers? Dr Steve White (second from left) and friends model the new look for *IBM's* men in suits.

Winn Schwartau's talk concerned Information Warfare. The growth of the information superhighway, in his opinion, has led to commensurately increased risks, with computers being both the weapons and the targets of those weapons. Schwartau argued for education and protection, a stance which reflects the concerns of many security personnel: with added connectivity comes added risk. Many now feel that the expansion of the *Internet* has been 'too far, too fast'.

Virus, Virus Everywhere

After a hard-earned (and welcomed) lunch break, the conference continued in two sessions, one chaired by Fridrik Skulason, the other by Rod Parkin. Skulason's technical stream opened with an unsettling vision from Vesselin Bontchev: future trends in virus writing.

The 4000+ viruses which exist at present grow by 3-5 daily, stated Bontchev. This poses problems for software developers, who must keep abreast of the epidemic as well as developing such techniques as heuristic and generic detection. Virus authoring packages, virus mutators, and viruses designed to target particular anti-virus products are other problem areas, as are false positives, which Bontchev views to be as problematic as real viruses. The next speaker, Mikko Hyppönen (*Data Fellows*) spoke on retroviruses, the viruses which target anti-virus products. Fortunately, his conclusion was that developers can take many precautions to ensure that their products do not become targets.

An active and vigorous open forum closed the technical stream, with many valid points raised. Bontchev put forward the view that scanners, with the ability to detect only known viruses, are inherently weak. Any scanner can be *made* to look good, asserted a delegate, if the 'right' test-set is used. On the subject of VXBBSs, the worrying scenario of viruses not in the wild being downloaded and released was raised.

Security Measures

The corporate stream, meanwhile, heard talks on principles of computer security (Martin Smith, *Kroll Associates)*, the *DTI* code of practice (Mike Jones, *DTI*), and key controls used to detect viruses (Linda Saxton, *Midland Bank*).

Smith placed responsibility for computer security squarely in the laps of users; a problem with people, not machines. His concluding thought was that 'awareness and training are the food and drink of security'. The following two speakers covered similar ground, illustrating key controls in computer security and virus protection. Ms Saxton summed up the afternoon's assertions in one succinct statement: 'For the future,' she declared, 'better technology may offer partial solutions - but people will decide our fate.'

The Next Instalment

Friday started somewhat later than the first day of the conference - after the late-night gala dinner, most people were pleased to have an extra hour's sleep!

The conference wasn't all play, play, play. Speakers and delegates settle down to some serious arguments about the future of the industry.

The day opened with a stimulating talk in both streams: David Ferbrache spoke on viruses on platforms other than the *IBM PC*; a subject about which, when compared with the PC arena, relatively little is known. However, as Ferbrache said, the first known computer virus in the wild, Elk Cloner, was written not for the PC but the *Apple II*. Threats are inherent in most operating systems: the *Amiga*, the *Atari*, the *Mac* and the *Acorn Archimedes* all have their own viruses. The multi-platform virus, which can be transmitted through different systems, is also a problem facing researchers and developers. Ferbrache's premise is that many techniques seen on the PC can be expected to spread to other platforms, and that invaluable lessons can be learned from such viruses.

Running parallel to this discourse, delegates at the technical stream were participating in one of the most interesting presentations of the conference. The talk, titled 'The generic virus writer', was presented by Sara Gordon, from *Indiana State University*. Gordon has spent many years researching the motivation behind those who write and distribute viruses, and has gathered large amounts of data on the subject, including comments from the Dark Avenger.

She outlined the results of a survey which she had made of virus writers. People from various age groups were polled, with case studies carried out in each area to try to determine common factors. Respondents were overwhelmingly male, the only female respondents being the girlfriend of a virus writer, and a female VXBBS SysOp.

Her conclusions were that, for the most part, virus writers conformed to the ethical norms for their age group. The exception to this generalisation was the adult virus author, stereotypically a loner, concerned with power issues and the injustice of society. Such a person, even if not an expert programmer himself, seems to expend considerable energy encouraging other, usually younger, people to write viruses.

Apart from the adult virus writer, Gordon believes that there is no 'homogeneous group to which the virus writer conforms', and that there are too many observable differences to

Rumours now abound that Alan Solomon and Jan Hruska are in fact twins, accidentally separated at birth. Here they prepare to establish which scanner has the highest hit rate.

be able to categorise them generically. In her opinion, most people become involved in this underworld through simple boredom and peer pressure, and although she conceded that legal means can and should, be used as part of any solution, her view was that enforcement of jurisdiction would prove in many cases virtually impossible - far better, she said, to give young people alternatives to antisocial actions (something which may be easier said than done).

Next, the *ITSEC* certification of anti-virus software, with its goals and achievements to date, was described by Chris Baxter. This is a UK government initiative with an ultimate aim of support and organisation by industry. It plans to evaluate products as a service rather than just software; i.e. as well as testing the effectiveness of the software, the company will be evaluated for its ability to maintain its standard. Areas to assess might include:

- whether the company is tracking the threat closely
- whether the threat is adequately understood
- whether the company responds effectively to the threat.

Tackling the Threat

The afternoon's corporate sessions opened with a presentation from Joe Norman, of *SGS Thomson*, on whether vendors are meeting users' needs. Norman's premise seems already to be becoming 'received wisdom': namely, that server-based anti-virus protection is at least as important as workstation-based measures.

Another highlight of the afternoon was Joe Wells' talk on viruses 'in the wild'. Wells, from *Symantec*, is in contact with many vendors and researchers, and maintains a list of which viruses have been found on users' machines. The result of this work is the 'Wildlist', which allows a user to identify which virus he has, even if the product used to detect it does not use a standard naming convention. One of the spin-offs from Wells' work is that the naming of common viruses is gradually being standardised across competing products.

Automatic extraction of computer virus signatures was the basis for Jeff Kephart's presentation. He and colleagues at *IBM* have developed a statistical method for automatic extraction of 'good' signatures from a virus. His premise is that any automatic task can be done as well by a computer as a person - but that a computer does it more quickly. This method raises the possibility that a computer encountering a previously-unknown virus could develop an 'antibody' to that virus without human intervention, cutting response time to a new virus to hours rather than days or weeks.

The Social Scene

As usual, many delegates came with partners, and the organisers ensured their entertainment while the rest of us worked: on Thursday, a sightseeing tour of Jersey was deemed 'most enjoyable and educational'. Delegates also managed to find 'time to play': Wednesday's informal dinner turned into a festive occasion - not surprising, as people greeted each other in person often for the first time since the last *VB* conference.

The gala dinner on Thursday was enjoyed by all: the theme was the *Blues Brothers*, and the hotel added to the fun by providing the ladies with feather boas; the men with fedoras and dark glasses - a relaxed start which set the tone for the evening. Entertainment throughout dinner was provided by a jazz band and a roving caricaturist [*who did **not** excel at flattering likenesses. Ed*].

Later, guests were regaled by Edwin Heath, the world's foremost hypnotist. Feelings were mixed as to the phenomenon's authenticity, but most agreed that those 'under hypnosis' were affected to some degree. Sadly, all pictures of those hypnotised mysteriously disappeared from the *Virus Bulletin* office before publication…

Thanks and Thoughts

The organisation team, not yet recovered from the exertions of *VB 94*, is already hard at work planning next year's event. Thanks are due to all those who helped with the conference, in particular Karen Richardson, Victoria Lammer, and Rosalyn Rega (*Expotel International Travel*): without their efforts, chaos would undoubtedly have reigned.

Special thanks go to Petra Duffield, the mastermind behind the *Virus Bulletin Conference*, who always ensures that things run flawlessly. Thanks also to the speakers, who gave their expertise and time, and finally, to the delegates themselves, who are the reason for the existence of the conference.

Discussions have already been taking place as to the venue and content of *VB 95*: if readers have suggestions, please contact *VB*; new ideas are always welcome. As for next year - keep your ears to the ground and your fingers at the keyboard; it won't be long before we let you know!