

## CONFERENCE REPORT

### Tram, Bam, Danke Schön

What better place to ponder the developments of the anti-virus industry, not to mention the German obsession with radishes and gravy, than the sumptuous surroundings of the Munich Park Hilton, venue for this year's *Virus Bulletin* conference? Over two hundred and fifty delegates, speakers and exhibitors from all over the world made VB'98 the biggest and, judging by the feedback, the most successful of our conferences to date.

*Data Fellows* (Finland) sponsored the delegates' badges, *NAI* (GmbH) the conference bags containing full proceedings on paper and CD, and a *Norman* (Norway) the VB'98 tee-shirts. A big thank you to all the sponsors who were instrumental in making VB'98 so conspicuously chic.

Weary German commuters waiting for the seven o'clock tram home on Wednesday evening may have been puzzled to see the cream of the world's anti-virus industry straggling along the twilight Munich streets in a disorganized crocodile. To add insult to injury, VB'98 appropriated the next three trams and set off sightseeing to the sounds of lederhosened 'oom-pah' and clinking glasses. The first was rather eclipsed by the last. Cheers to *Sophos*, sponsor of this welcome drinks reception with a difference.

On Thursday morning we were treated to the full glory of the sun on the Alps at breakfast on the fifteenth floor. The location of the VB'98 dining rooms presented something of a challenge due to the smooth velocity of the elevator which left some of us fighting an odd combination of travel sickness and vertigo, not helped by the previous evening's surfeit of schnapps. Nonetheless, there was a full and enthusiastic turnout for VB editor Nick FitzGerald's opening address – 'What a difference a year makes' – a talk which set the tone for the entire conference.



Carey 'Muffin' Nachenberg preparing his paper on heuristic virus detection.

Nick's presentation encompassed a range of issues and perspectives, considering the major events of the last year along with predictions for the future of both development and developers. He highlighted the importance of the industry's awareness that anti-virus is a service not a product, and

introduced the idea of a united front of developers and vendors – to be debated up to the last minutes of the speakers' panel on Friday evening.

He went on to cover the mutating corporate face of the industry and new, serious developments in virus creation like CIH. Further topics included the increase in Win32 expertise, 'improved' macro techniques, the net-ification of viruses, 'monster' viruses, and viral 'nastygrams'. He remarked on the emergence of new classes of host – *mIRC SCRIPT.INI* viruses, Access macro viruses, cross platform and Java viruses. Lastly, he touched on non-virus developments – the apparent 'disappearance' of Trojans, new hoaxes like Bloat and network backdoors.

While representatives from all the major international anti-virus companies exhibited, they formed a noticeably smaller crowd than last year, reflecting the effect of recent mergers and acquisitions on vendor numbers. There was unprecedented press presence this year, from publications including *Chip*, *Focus*, and *Secure Computing*. Independent journalists from all over Europe also attended.

From the off, *NAI*'s Jimmy Kuo's keynote address 'Add Common Sense, Stir' promised to be challenging and controversial. He discussed several issues that were the focus of later sessions in arguing that an overly-rigorous, 'scientific' approach to product design decisions could be detrimental to the industry's clients.

The papers were presented in two streams – corporate and technical. Previous *VB* editors Ian Whalley and Richard Ford looked at the problems and pitfalls of certification schemes and general anti-virus software reviews. Meanwhile, Péter Ször presented a detailed and well-received paper on Win32-specific virus threats. Rounding off Thursday's morning session, Robert Stroud tracked evolutions in the virus scene and the implications of the changing threat for anti-virus and security policies while Carey Nachenberg discussed heuristic virus detection.

Randy Abrams then described the lengths to which his team go to ensure *Microsoft* does not ship known viruses in retail and digitally-signed software. Unable to influence the design and coding teams to use 'clean room' techniques leaves his Product Release Services group in a similar position to that which the magazine cover CD people face.

Christine Orshesky's paper followed, with a detailed description of defining, testing and choosing anti-virus software, comparing the procedure to that of purchasing a new car. In the technical stream, securing your Web browsers through proper configuration once you understand the threats, and by using 'anti-vandal' software were the themes discussed by John Morar and Dave Chess, and Shimon Gruper, respectively.

After tea, issues of dealing with anti-virus software in large and diverse corporate and university environments were tackled in the corporate stream by Ian Clark and Shawn Campbell, and Dave Phillips, while the technical stream grappled with macro virus issues. Jakub Kaminski investigated 'disappearing macros' due to shortcomings in the compatibility of WordBasic and VBA5 and Vesselin Bontchev warned of the 'evils' of macro virus upconversion if practised by anti-virus researchers.

The gala dinner, generously sponsored by *Network Associates* (USA) was a huge success, with interactive entertainment and a superlative pianist. Highlights included the mime clown's unrehearsed double act with one of the *Sophos* directors and four seemingly consecutive renditions of Barry Manilow's 'Mandy' requested by the less than voguish Assistant Editor [*I'm pleased she wrote that. Ed.*]. In a departure from the norm, an extempore dance session saw the hard core element boogie the night away.

A later start with only one session before coffee saw a quite respectable turnout to the first session on Friday morning. Daniel Diefenderfer pointed out some of the 'institutional' barriers to effective anti-virus software maintenance thrown up *within* a company and how to work around some of them. The technical stream heard Marko Helenius present the details of some of the automated virus replication and software testing systems he has developed for use in the University of Tampere anti-virus software evaluations.

After the break Paul Ducklin discussed strategies for catching viruses at their entry point to organizations, and Sarah Gordon and Dave Chess presented their research on 'the truth about Trojans on the Internet'. Meantime, attendees of the corporate stream were treated to Cindy Snow's description of the development processes involved in the evolution of *Intel's LANDesk Virus Protect*. This was followed by Bruce Burrell's exhaustive [*and exhausting, for him! Ed.*] study of the appearance of viruses in the WildList relative to their initial detection.

Postprandial proceedings kicked off with David Aubrey-Jones' consideration of the issues surrounding email encryption and the technical problems this can pose for email virus scanners. He was succeeded by Emily Hawthorn's presentation on the significance of mail gateway scanners. *VB* conference veteran Steve White reflected, for the technical stream, on problems that are still unresolved despite more than a decade of anti-virus research. Then Mikko Hyppönen, newly coiffured, described an approach to macro virus detection that alerts the presence of non-certified macros rather than that of known viral ones.

The final technical session saw Stephen Trilling contemplating the pros and cons of various approaches to incremental product updates. Next door in the corporate stream,

Shane Coursen set the stage for a lively speakers' panel session during his paper on WildList developments with the suggestion that the *WildList Organization (WLO)* should provide reviewers with verified virus samples.

The speakers' session at the close of the conference proved popular and controversial – Nick represented *VB*, Carey Nachenberg *Symantec*, Steve White *IBM*, Dmitry Gryaznov *NAI*, and Paul Ducklin *Sophos*. Jan Hruska presided over a very enthusiastic full house. Shane Coursen, Ian Whalley and Richard Ford met Vesselin Bontchev head on in the debate over the *WLO* providing samples to reviewers.

Paul Ducklin reiterated the value of presenting a solid team of developers and vendors, despite differences in marketing and development techniques and priorities. The audience appeared to be surprised at the level of technical cooperation between anti-virus companies, given the extent of inter-marketroid bickering. It seemed to be a staple theme of this year's conference that the 'you' and 'us' developer/vendor dichotomy be screened by a manifestation of unity from the 'same side'.

On behalf of the whole team, big thank-yous go to several people. Petra Duffield manages to outdo herself every year, and *VB'98* went especially smoothly thanks to her organizational expertise. A big thank you Pet from everyone in your corner. Thanks are also due to Dan 'Roger Irrelevant' Trotman, making his memorable debut as a conference helper along with the new conference coordinator and subscriptions manager Jo Peck.

Kim and Müsli, so cheerful, professional and polished every year, were joined by newcomer Sarah – all three must be congratulated for their invaluable and efficient help. Thanks also to 'Big Rich' for driving all the conference material over and helping to set it up. The conference organizers would like to voice their appreciation for the boys from Gearhouse, who were responsible for the audio-visual equipment and presentations. They managed another superb job and their group rendition of 'Yellow Submarine' at the gala dinner will become the stuff of future legend.

Last but not least, thank you to all the staff at the Munich Park Hilton, especially Andreas and Martin who managed to maintain their composure and patience despite the logistics of getting two hundred and fifty delegates up fifteen floors twice a day.

Special mentions to – *ICSA's* Scott Markle and his remarkable talent for spotting biscuits at a thousand paces. Marta Olafsdottir for her professionally rendered Lloyd Webber numbers in the piano bar, Svein Meland and his wife for being dazzling in authentic Norwegian costume, and last but not least, to Stephen Trilling for his very generous offering of a million *Symantec* dollars to shave the editor's beard off for charity. [*No joy I'm afraid. Ed.*]



*NAI's* Dmitry Gryaznov takes centre stage at the gala dinner.