INSIGHT

Fighting Fire with Fire

Megan Palfrey

In 1989, Joe Wells encountered his first virus: Jerusalem. Wells disassembled the virus, and from that moment onward, has been intrigued by the properties of these small pieces of self-replicating code. In less than five years from this first incident, Wells has become an expert on computer viruses, and is now partly responsible for the development of one of the best-known anti-virus products, *NAV 3.0*.

Genesis

Wells' first brush with computer viruses did not immediately take him into a career in the data security industry. After leaving his current job, he spent eighteen months working as research editor at a business magazine. During that time, his interest in viruses remained a hobby - but for the fact that he started to review anti-virus products, this might have remained the case.

Unsurprisingly, when writing reviews, his experiences with vendors ranged from one extreme to the other. He recalled two companies sending him their 'latest' viruses along with their 'latest' scanners. Feeling obliged to be fair to other anti-virus companies, Wells sent the viruses he had received to two other vendors, to allow them to amend their products. Although they gratefully accepted the viruses, they felt themselves ethically bound not to release their own libraries, even if it meant a better score in a review of their product.

Even at those early stages, the ethics of 'distributing' viruses was not confined to the anti-virus industry. Wells remembers a cry for help from a woman who asked him to examine her computer after she had had a disagreement with the 'consultant' whom she had employed to set up her system. 'He insisted on teaching her *WordStar*, but she wanted *WordPerfect.*' recollects Wells. 'She fired him, but he returned once to "finish a setup". He rebooted her machine from a floppy disk and left. Two days later, she was greeted by a message that Disk Killer was "processing" her drive. I gathered evidence for her, but she was afraid to pursue it. It seemed that other "virus threats" were also involved.'

A Growing Problem

It was not long after this that *Certus* and *Microcom*, the companies which had not passed on any virus samples, approached Wells with job offers. Although he accepted *Certus'* offer, his contact from *Microcom*, Glenn Jordan, became his closest friend and ally in the industry.

Wells started at *Certus* in 1991, as a 'Virus Specialist'. Soon after his arrival there, it was decided that a new product was needed, which would meet the demands of a burgeoning problem: thus, *Novi* was conceived. His involvement with the product concerned virus-specific detection, file repair, and information systems. Even at this stage, he was more heavily involved with the research side than with programming.

> *"Less than one percent of homes burn down, but I would recommend that all homes have a smoke detector"*

Among the many tasks Wells was assigned at *Certus*, he was asked to develop alliances within the anti-virus industry. This led to him becoming involved with Ken van Wyk's ad hoc group, which cooperated in disseminating anti-virus knowledge. In 1992, they amalgamated with *CARO* (*Computer Anti-Virus Research Organisation*).

Wells believes that the *CARO* cooperative is one of the most useful in the industry: 'My relationship with *CARO* has proven symbiotic, and is quite satisfying, due to my fact-processing addiction. Its strength lies in the fact that, like a good marriage or friendship, participants are there for what they can add, rather than what they can get out of it. It is founded entirely on trust.'

Mix and Match

Certus was acquired by *Symantec* in late 1992, and many of the techniques which had been developed for *Novi* went into *Norton Anti-Virus* (*NAV*) . The addition of the *Peter Norton Group's* utility libraries, as well as the availability of a staff of programmers and quality assurance personnel beyond the means of *Certus*, greatly enhanced the systems being developed for *Novi*. Wells was heavily involved in the development of *NAV3.0*, which (under the name of 'virus sensor') has *Novi's* file watch built into it. The heart of the *NAV 3.0*'s main scanning engine also has a *Novi* pedigree: it is an enhancement of *Novi's* 'warp drive'.

As with *Novi*, Wells' responsibilities involved virus-specific systems. The basic design of the detection, repair, and information systems is his, although shaped and enhanced by the work of many other programmers.

Symantec's interest in the anti-virus market is hardly surprising, according to Wells. He believes that the anti-virus market is growing in proportion to the virus problem, and as the computer universe accepts viruses more as a fact of life. Many companies, he says, are already budgeting for multiple anti-virus products: 'Most people with whom I deal already have more than one anti-virus product, as they have more than one editor, more than one backup, etc. As this

becomes the norm, anti-virus product concordance becomes more of an issue. Fortunately, nearly all anti-virus product developers (except Central Point) have accepted responsibility for keeping their product compatible with others.'

Although *Symantec* is a far bigger organisation than *Certus*, Wells is still very much in touch with the needs and problems of the user as well as technical developments. Wells' job description at *Symantec*, according to his manager Jimmy Kuo, is 'walking virus encyclopaedia'. A large part of his job ('Happily!' says Wells) still consists of answering virus questions and helping users.

Views on Viruses

'I tend to lean more towards research than development,' said Wells, 'but only if the research accomplishes something useful. I once heard knowledge likened to a pool of water. Without constant input it stagnates, and without someone using it, it is wasted. As a research editor and virus researcher, my work seems always to revolve around collecting, analysing, coordinating, collating, and releasing information for others to use.'

He feels that viruses are still less than a 'one percent problem': less than one percent of known viruses are common and are on less than one percent of machines - 'this is not to say that the problem is not critical. Less than one percent of homes burn down, but I would recommend that all homes have a smoke detector,' says Wells. Although the glut of new viruses is quite out of hand, the number in the wild is still just over 100 and therefore, he feels, eminently controllable. Most anti-virus reviewers today are 'stuck in the scan age', according to Wells, and have no concept of how to test and review integrity systems. 'So, they keep feeding their readers the lie that detection rate is everything.'

He sees prevention as being more effective than cure: when Wells receives a new virus, he infects the system to see what it does, then uses *NAV's* inoculation system to detect and repair all the infections. This, in his view, is quick, easy, and effective. He believes that integrity systems will be the way forward into the next century, although an anti-virus product should at the very least know all currently in-the-wild viruses. It should be able to clean up a system, and then install a good integrity management system.

'After installation,' he observed, 'the combination real-time and interactive integrity systems can handle the new viruses that appear.' He believes that anti-virus products will develop along both generic and specific lines, but with virus-specific detection being crucial only for installing a more intelligent system. Wells views detection of rarer viruses as less important, and able to be done generically: 'We recently received 151 new viruses from a researcher, and detected 150 of them with a current "fuzzy" signature.'

Education is a useful medium in the fight, but although it helps users deal intelligently with viruses, it is not the whole solution: 'Education may limit the number of virus disasters, but not the number of incidents,' says Wells. 'It should be focused towards preparing users, dispelling myths, and maybe teaching computer ethics.'

Personal Points

Wells plans to continue in virus research, and hopes to expand his informational role in the field, by pursuing more projects such as the 'In the Wild' and 'Frequency' lists which he currently collates. He believes that misinformation and bad advice is still widespread: 'Just yesterday I saw a horrifying post on *CompuServe*. A virus "expert" was telling a user to use FDISK /MBR to remove Monkey, which would leave the disk with scrambled partition information. The same trick is often suggested to remove Form, which doesn't infect the MBR at all!'

Although he is vehement in his belief that viruses are a problem which must be controlled by any and every means possible, he also feels that the writing and perpetration of viruses is an ethical issue, not a legal one; therefore, he does not view virus writing as a crime. However, he would probably support legislation about virus programming and virus damages.

"products will develop along both generic and specific lines, with virus-specific detection being crucial only for installing a more intelligent system"

'Even if such legislation failed to pass,' he said, 'at least it would succeed in raising a fact-based awareness of the virus problem. The ERA [Equal Rights Amendment] failed to pass in the USA, but the discussions surrounding it did much to increase public knowledge and change attitudes about real problems.'

'All in all,' said Wells, 'the perspective I've developed in my career is perhaps a bit odd. As a "techie", I still use DEBUG more than any other tool, but when I read a review that rates a product highly because of the interface, the editor in me has to nod in agreement. For *MIS* people who have *Windows* on 80% of their systems and viruses on few, compatibility and usability are the dominant prerequisites. That perspective has been acquired both from the views of a small company, trying to survive, and from a huge corporation, trying to thrive - two very different vantage points. I liked the family feel of a small company like *Certus*, and I miss that. But, despite the corporate atmosphere, I prefer the reach of a company as large as *Symantec*, simply because the information I process now can benefit far more people.'

Wells fights fire with fire, bringing his expertise and the wealth of his experience to bear upon the problems of the user. Can he continue to do so? 'Yes,' he promised.

VIRUS BULLETIN **©1994 Virus Bulletin Ltd, 21 The Quadrant, Abingdon, Oxfordshire, OX14 3YS, England. Tel +44 (0)235 555139. /90/$0.00+2.50**