INSIGHT

Once a Researcher…

There is a farm in upstate New York which is avoided 'like the plague' by strangers to the area: there are signs posted on the boundaries that warn of live viruses on the property. The farm is Virus Acres; it is owned by a man who enjoys a joke: Ross Greenberg.

Despite the fact that he has kept a low profile lately, Greenberg is a familiar name to many virus researchers, and the author of *Flushot+* and *Virex PC*. However, the former is now defunct, and the latter no longer one of the major players. So where has he been, and what has he been doing?

Being There

Chameleon is a word one could use to describe this man: change seems to be a constant in his life; from student to media person to programmer to anti-virus researcher, once more to programmer, and who knows where from here?

He comes from what he calls a typical middle class, Long Island, Jewish background. His mother was a dental assistant; his father was an engineer who instilled in Greenberg a passion for seeing how things worked: 'My father made sure that, whatever I took apart, I put together again. I never got the opportunity of throwing things out,' he recalled. 'It was "Keep with it until you put it back together" – and I did!'

This practical childhood did not prepare him very well for a disappointing sojourn at university: 'I went to *Stoneybrook*, New York's state university, to study Physics, mathematics, and philosophy. I never did get around to graduating – in 1978, my senior year, I looked around at what kind of job I could get, and saw that a physicist working at *Brookhaven National Labs* with 15 years of experience and two PhDs was worth about $17,000 a year. So, I took a job with *MetroMedia TV*, a local network, starting at that salary!'

Greenberg's responsibilities at *MetroMedia* lay in setting up PC to PC communications programs to coordinate radio and TV advertising, so the company could gauge how much money they were either making or losing: he stayed a mere eight months, going from there to private consultancy.

'Communications by that time had become a speciality of mine,' he explained. 'There were few people around who could do it. If you had a spell at a thing, you became a specialist. I could charge top dollar, which was sort of fun!'

Flushot: Pluses and Minuses

Gradually, Greenberg began to branch out into more general things, writing programs. He remembers a person who was beta testing one of his products sending him a note: '…from a fellow named Ken van Wyk. That note, which he put up on the Net, said that he was being attacked by – I think he called it a virus; a Lehigh virus.

'I thought that this was really horrible, and that it would affect the on-line community adversely, so I put out a fix; a program called *Flushot* – it was downloaded astoundingly quickly, and I started getting tech support calls. Then, as it became bigger, I put it out as shareware – I think it cost $14.00 all-in – and the next thing you know people are buying it, and making demands. That was in the mid-1980s.

'In those days,' he said, 'there were no scanners. I created a behaviour blocker based on what I was told about the virus. I think *McAfee* was the first to produce a scanner. A fight soon broke out between the anti-virus people over scanners and behaviour blockers. The scanner won, for many reasons, but I think behaviour blockers are more effective. They fight the unknowns – scanners do diddley-squat for unknowns!'

Virex PC

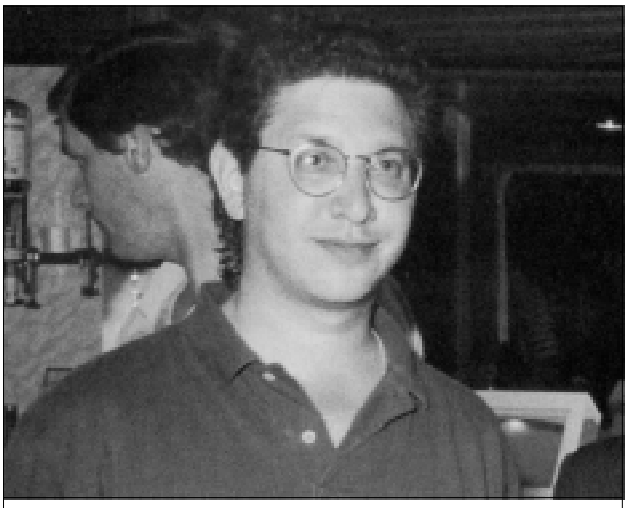
Soon after, Greenberg was contacted by a company called *HJC Software*: they had a *Macintosh* anti-virus product called *Virex* which they wanted to develop for the PC, and believed Greenberg could do it. Dealings with *HJC* were, for Greenberg, less than ideal, and the company sold out to *Microcom*: 'They marketed it into the ground,' he recalled. 'When I threatened to sue for breach of contract, they offloaded it onto *Datawatch*. I think they noticed *Virex PC* still had its head above ground, so pushed it down more.'

'Anything I had to say about the product,' he went on, 'was rejected by *Microcom* and *Datawatch*. They had a distinctive 'Not-invented-here' paranoia which prevented them ever taking suggestions from me. So, Glenn (Jordan, formerly of *Datawatch*) and I would confer and figure out how he could present them in a manner more palatable to their paranoia. He did a wonderful job for *Virex PC*.'

Leaving the Rat-race

Subsequent to this, Greenberg decided to distance himself both from *Virex PC* and the City, and moved to a farm in upstate New York. 'I haven't been doing much virus work,' he said. 'I've been developing telecommunications programs, in particular a shareware product, *RamNet UUCP*. It's a background program that talks to UUCP protocol. They came out commercially at $198.00, but I didn't like the idea of having to do the marketing and advertising, so I dropped the price to $49.00. Commercially, it's meeting my expectations – and they are that I can retire in about a year!

'Since I haven't been so active in the anti-virus world,' he went on, 'it's been interesting to see how short-term people's memories are. I've been out of the picture for three years or so,



Ross Greenberg, author of *Flushot*, *Virex PC*, and *RamNet UUCP*: a man of diverse interests.

and at *VB 95*, I noticed that some people hadn't heard of my products. All the *CARO* members know me, of course, but some of them don't know what I've been doing.'

Carrots and Other Nourishment

Greenberg is still, to an extent, an active member of *CARO*; though, as he stated, there is no membership per se: '*CARO*,' he asserted, 'is a group of people loosely affiliated who share common interests, involving computer viruses and beer drinking! I share my knowledge and expertise with fellow anti-virus people. This is what *CARO* is about. They are more active in the field than me, though – when a new virus comes in, they jump on it straight away… I do it when I get around to it. Often, when that time comes, it's been done!'

Greenberg sees no new techniques in virus writing: 'Polymorphism was one… Interrupt stripping was another… Big deal! The first fifty viruses I tore apart were fascinating, each and every one of them. Of the next couple of hundred, some were mildly interesting, most were boring. The next thousand or so were pretty tedious. The ones that came later – boy, I was glad I was out of the business. Someone had to tear them apart, and I didn't want to.'

Not a single virus, in his opinion, stands out as an exemplary piece of coding, though some he recalls for other reasons: 'DBase was interesting… that was the first virus to screw around with data. Datacrime I remember because I was interviewed by five TV stations, and only one – *CNN* – had the guts to play what I'd said; that it was a non-problem. I didn't get any airtime with the major networks,' he related, 'because I wouldn't say the sky was falling. Unfortunately, media hype has made some vendors extraordinarily rich.'

The Legality of it All

Here in the UK, a young man will soon appear in court for sentencing after having been charged with eleven offences under the Computer Misuse Act. He is charged with writing viruses, and with inciting others to do the same. Could a similar thing happen in the USA? 'There was one person, PhiberOptik, who was sent to jail,' mused Greenberg. 'When he came out, he was a folk hero; everybody celebrated him because he didn't do anything "all that bad". So I don't know if prison is the right idea.

'Maybe a better punishment for that kind of person would be to forbid him ever using a computer again, or for a fixed period of time, and not to allow him to hold a job using computers… I'm not sure how it could be enforced, but being taken away from something he's addicted to would have more effect on the individual than being put in prison.'

Legal redress, he feels, has its place, but only if it is done in a very public way will it have any kind of prohibitive effect on virus writers: 'It's sad,' he said. 'There's this thing called the On-line World, which I loved, and the virus writers were destroying it. It used to be if someone gave you a cool program you didn't have to worry about it … now you do.'

The Next Act

Greenberg thinks that the next new wave of viruses to hit will be OS-orientated; *Windows 95* and *OS/2* viruses which will take advantage of the holes in those operating systems. Indeed, he thinks the only surprising thing about the infamous Concept virus is that it took so long to be released.

The future for detection software, he believes, will not lie much longer with scanners: 'The final solution,' he stated, 'will be a hook in the operating system. Scanners will be very useful for uniquely identifying the virus, but I think they'll be used in conjunction with heuristics. There will also be integrity checking; things like that.'

He feels strongly about the fact that many smaller companies are being swallowed up by the giant conglomerates: 'Competition is good. Seeing new and interesting technology disappear stinks. Companies are bought out,' he explained, 'then the new owners don't want to develop the ideas further, and they are lost forever. Unfortunately, with the best product in the world, if it's not marketed well, it'll be lost. Only the bigger companies have the money to keep their products exposed out there every day. That's where shareware, used properly, can be the great equalizer.'

Although Greenberg is no longer disassembling viruses daily, he still takes an active interest in the anti-virus world, and is considering returning to the fray; however, he is somewhat put off by the antics of certain vendors, whom he sees as less than ethical in their tactics and methods.

In the meantime, life goes on at Virus Acres: Greenberg's seven-year-old daughter has just acquired a brother ('mother fine, child fine, father entirely exhausted!' read the announcement). Whatever route Greenberg eventually decides to take, his expertise and enthusiasm will certainly help to make his task easier, and should he return to full-time virus research, his knowledge and ideas will be heartily welcomed.