FEATURE

Regina v Christopher Pile: The Inside Story

Jim Bates

With the Black Baron case still relatively fresh in the minds of computer users, now is a good time to put the facts on record. As I became involved at an early stage, I can speak with some authority on what happened and how the case against Christopher Pile was built.

Preliminary Enquiries

On 13 July 1994, the Police obtained a warrant to search Pile's home, under Section 14 of the *Computer Misuse Act 1990*. That search revealed an old *Sinclair Spectrum* computer in a bedroom wardrobe: nothing more. Pile affected disinterest in anything to do with computers.

His bedroom did, however, contain a table boasting a newly-installed telephone extension cable. The Police were fairly sure that Pile knew they would be calling, so such a large 'computer-shaped hole' was suspicious. Pile was cautioned, arrested and taken to the Charles Cross Police Station in Plymouth (southwest England).

I then went to another address in Plymouth where the police were conducting a simultaneous search in connection with the same enquiry. Here, a quantity of computer equipment was found in the living room, which was labelled, packed, and transported to the Police station.

In a bedroom at the same address, on top of a wardrobe, a box containing a *Tandon* computer, keyboard, modem, mouse and around fifty diskettes was found. The occupant of the house, on being questioned, indicated that the *Tandon* belonged to a friend, and was merely being stored there. This too, along with the occupant, was taken to the Police Station. The occupant was subsequently cleared of involvement in Pile's activities.

At the police station, both men (each initially unaware of the presence of the other) were questioned further. Enquiries centred around a known series of telephone accesses to certain BBSs around the UK and the uploading of virus-infected programs to them. During preliminary questioning, Pile denied any recent knowledge of computers, saying he had disposed of his machine some time around the previous November (1993).

It is my understanding that the police at this stage already had sufficient evidence to charge Christopher Pile with offences under the *Computer Misuse Act* and were anxious to complete their enquiries before a complete list of formal charges was preferred.

Analysing the Equipment

Meanwhile, I was creating image copies of the machine's fixed and floppy disks before beginning initial examination of their content and structure. Preliminary analysis of the first computer showed it to be a standard machine in a state indicating normal use by someone involved in programming graphic images for computer games. The *Tandon*, however, had been completely defragmented and wiped, destroying almost all traces of previous activity.

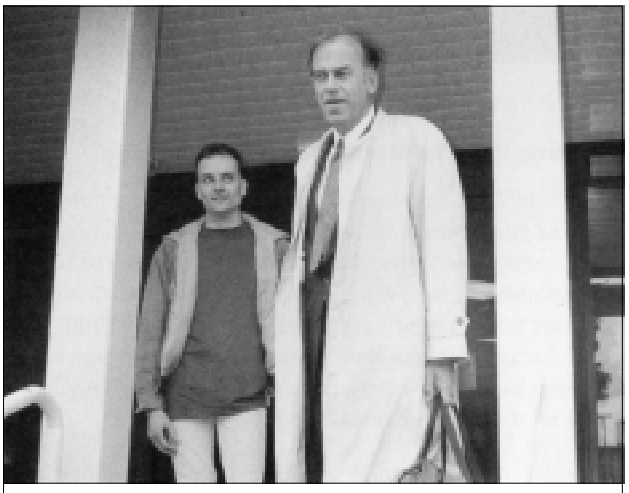
This was extremely suspicious, and a more detailed examination was begun. Fairly quickly, this revealed two document files, both of which were job applications in the name of Christopher Pile name, thus establishing that the machine was probably Pile's. The files were printed off and given to the investigating officers.

When imaging of the floppy disks was completed, they were examined, and shown to be commercial disks for *Windows*, *MS-DOS*, a modem, and mouse and printer drivers. Image analysis was then begun: the first stage highlighted a file on a manufacturer's diskette found in the mouse box. The file, MOUSE.DAT, showed sufficient indication of being unusual that it was marked for further analysis. It had the same date and time as the other files on the disk, and closer examination revealed that it contained encrypted information.

The Accusations Admitted

The immediate results of this analysis, together with the printouts, were passed to the investigating officers, who began a second interview with Pile. He denied any knowledge of the computer until he was shown the job application

Virus expert Jim Bates, whose testimony (along with police efforts) was instrumental in obtaining a conviction.



Pile with his solicitor on the steps of Plymouth Crown Court, after being charged with distribution of viruses.

documents. At that point he asked for a private word with his solicitor and subsequently admitted owning the machine, although he still denied any knowledge of viruses.

Questions were then put to him concerning telephone calls made from his address over a period of time to various BBSs in the UK. Pile eventually admitted making these calls on his computer, but although the timing of the calls was a strong indication that he was responsible for certain infected uploads, he continued to deny involvement with virus code.

Eventually, Pile was asked about the MOUSE.DAT file on the floppy, at which stage he asked to speak with his solicitor. On resuming the interview, he admitted everything, and gave the Police the password of the encrypted file. On decryption, the file was found to contain source code to a number of viruses, as well as documents by Pile and others which were directly concerned with viruses. After making his confession, Pile was released on bail while further enquiries were conducted.

This concluded the initial investigation: I returned to my office with copies of all the images to analyse. I was later asked to produce a report, together with any related material I could find, on the contents of the file MOUSE.DAT. There were small evidential traces on the *Tandon*: in the light of Pile's confession, analysis of these was not required.

I wrote a report on the evidence and sent this to the Police. Over the next few months I received a regular supply of virus-infected files sent to me by the Police from various complainants. Each of these files had to be confirmed as one of Pile's creations and analysed to reveal the value of the generation number stored within them.

At this time, a number of reports of infection by Pathogen or Queeg were reported from various quarters, then denied: some complainants were presumably being gagged by their companies. Happily, however, many specimens were received from other sources, and were analysed as the evidence mounted.

Pile was interviewed further by the Police, and ten charges were framed under the *Computer Misuse Act*: five of unauthorised access, five of unauthorised modification. The trial date was set for May 1995 at Plymouth Crown Court.

Approaching Sentencing

As the papers were passed to Counsel before the trial, a further charge of incitement was added. At the trial the defence objected to the introduction of the charge of incitement, but the judge allowed it to stand. Pile pleaded guilty to all eleven charges.

The defence then applied for permission to commission their own technical report on the viruses so that this could be presented before sentencing. This was allowed, and Pile was remanded on conditional bail pending the setting of a date for sentencing.

In the interim, efforts were made to confirm the existence overseas of the viruses and the file SMEG03.ZIP – in this task, I had some assistance from other anti-virus researchers. Vesselin Bontchev helped with a statement confirming SMEG's existence on the continent, and other enquiries confirmed that it had been spread fairly rapidly and widely amongst virus exchange BBSs in various countries.

"the judge considered that the distribution of (viruses) was certainly the most serious charge brought before him"

Meanwhile, I continued to analyse examples of infection by these viruses. Amongst these was one from a Nottinghamshire college which had suffered quite severely and exhibited the highest generation number so far found – 27. This validated my assertion that continued infections would show increasing generation numbers until the destructive payload was delivered (generation 31).

In all, I disassembled and analysed over sixty specimens in connection with this case. The viruses were relatively simple, used no new techniques and would have been easily identifiable on their own. The polymorphic code was more devious, but in concept rather than in execution.

The defence technical report was produced by a Mr John Boarder, who, though displaying an impressive academic record in various fields of computing, had no experience of virus code or its effects in the real world. I produced a fifteen-page supplementary report detailing technical analysis of additional complaints, and highlighting inconsistencies and inaccuracies in Mr Boarder's report.

A date of 17 November at Exeter Crown Court was set for the hearing, at which it was expected that Mr Boarder and I would be questioned. However, on that date, after I had been examined and cross-examined, the defence counsel rose and

announced that although Mr Boarder was in court and had heard my evidence refuting his conclusions, he had nothing to add to his report and would not take the stand.

It then only remained for Judge Jeremy Griggs to adjourn the proceedings before returning to announce the sentences. On each of the ten charges, Pile was sentenced to six months imprisonment, to run concurrently. On the incitement charge, as it involved the SMEG polymorphic engine and indefinite proliferation of polymorphic virus production by other virus writers, the judge took a more serious view, sentencing Pile to twelve months, to run consecutive to the other sentences. So, Pile went to prison for eighteen months. Pile's solicitor later indicated an appeal might be considered: I am not aware that any appeal has since been filed.

The Implications

This landmark case has been interesting for many reasons; first, for the co-operation between the *Metropolitan Police Computer Crime Unit* and Devon and Cornwall Constabulary's Fraud Squad, which worked extremely effectively in co-ordinating enquiries both in the UK and overseas. Second, there was a direct link in the first nine charges between the defendant and the complainant: Pile was shown to have uploaded an infected file to a BBS; and the complainant was shown to have downloaded the same file, suffering virus infection as a result.

In the tenth charge, the situation was different. The complainant, *Microprose Limited* (a software publishing house) had been infected by Pathogen. The infection came from an outside source with no connection to any BBS known to have been accessed by Pile. The charge was the only one in which there was no direct link with the defendant other than the virus itself. This shows that, if someone writes a virus and someone else becomes infected by it, it is not essential that the link between the writer and the victim should be proven: presence and identification of the virus is enough.

Most significant of all was the sentence attracted by the incitement charge. This was concerned with the distribution of the polymorphic engine and its associated files. Even though Pile tried to suggest that this had beneficial uses, the judge considered that the distribution of such material into the world-wide computer communications network was certainly the most serious charge brought before him.

The Police can in future be expected to keep a much keener eye on the activities of the virus exchange BBSs, as well as distribution of certain books on virus writing techniques. There are those who think that the *Computer Misuse Act* is too weak to deal effectively with virus writers and distributors: this case has certainly strengthened it.

I cannot speak highly enough of the dedication and efficiency of the officers involved in this case, from initial collection of evidence, through search and seizure operations, to the series of interviews culminating in Pile's confession. I consider myself privileged to have worked with such men.