# Operation Dabble

# Hackers tap in to justice

*By Detective Sergeant Ken Day*

The conviction during 1993 of three computer 'hackers' has proved a milestone for computer crime investigation in Australia.

The success of Operation Dabble was the result of extensive efforts by the International Division, Telecommunication Interception Branch, Department of Public Prosecutions, Assistant Commissioner for Southern Region, Wal Williams (now retired), members of Southern Region Fraud and General Crime Division and members from the Southern Region Network Administration Branch.

This combined effort resulted in the detection, investigation and subsequent prosecution of a group of computer hackers known as The Realm. These offenders were charged with unlawfully accessing computer networks in Australia and the USA. Arrested on April 2, 1990 all were convicted in 1993 on various counts of computer crime offences in the Melbourne County Court.

Operation Dabble commenced on the April 17, 1989 after information received from the US Secret Service which alleged that an Australian hacker known as 'Phoenix'was actively attacking commercial, military and educational/research networks in the US. The activities of 'Phoenix' became a public issue in the US as his criminal acts became front-page news in the *New York Times* and were major bulletins in prime-time television news.

The environment in which this investigation was commenced was a difficult one. All that was known at the start was that an Australian citizen, only known then as 'Phoenix', was hacking into USA networks. This investigation was given a high priority as 'Phoenix', from the confines of Australia, was causing criminal damage in the USA. The AFP had an international obligation, both legal and moral, to stop 'Phoenix'.

On receipt of the information from the US Secret Service, an intelligence probe was commenced. At that time the AFP did not have any jurisdiction to prosecute 'Phoenix'. It was not until late July 1989, when the Commonwealth computer crime legislation was enacted, that the AFP had jurisdiction to investigate and prosecute 'Phoenix'.

The initial probe identified 'Phoenix' and other co-offenders. The three accused being investigated were:

Nahshon Even-Chaim alias 'Phoenix' (born May 28, 1971);

Richard Martin Jones alias 'Electron' (born August 22, 1969); and

David John Woodcock alias 'Nom' (born April 25, 1968).

'Phoenix', 'Nom' and 'Electron' all belonged to a group the called 'The Realm' and it was this group that became the target of Operation Dabble. Investigations into this group resulted in the gathering of sufficient information to apply for a telephone intercept on the two telephone lines used by 'Phoenix' which were commenced on January 24, 1990.

The telephone intercepts provided both verbal conversations and captured analogue demodulated computer data signals. The AFP pioneered the capturing of computer signals from telephone intercepts and their conversion to readable signals. This form of evidence gathering proved to be vital in the prosecution case against The Realm.

The intercepted data proved that 'Phoenix' and his co-accused were breaking into computer networks in Australia and the North American continent. During the intercept, the AFP was able to capture approximately one month of computer data transmissions. During the course of monitoring, a large number of sites were identified which 'Phoenix' had unlawfully accessed but considering that the AFP had only a one-month snapshot of what 'Phoenix' was up to there is no way of estimating the extent of his activities. It could only be guessed that it was extensive.

Evidence showed that as a general rule 'Phoenix' would first access a university and lose himself in the computer traffic. Once he believed he was un-noticed he would then 'jump' from that location to his intended target. Those targets at the time of monitoring were primarily military, educational or research organisations.

'Phoenix' stated in court that he was only hacking for the betterment of mankind. He stated that by identifying security weakness he was alerting administrators to security problems. This argument holds no credence as the intercepted material clearly proved that Phoenix had no remorse for the effects of his acts.

It can only be imagined what may have happened if Phoenix had been under the control of a serious criminal or political agent. This did not occur, but none-the-less he caused considerable damage through his activities. For example, he deleted the entire inventory records of a Texan company known as Execom. The company also believed that 'Phoenix' had modified Execom's accounting records. This was not so, but for a time it was thought that the company would have to be liquidated due to the inability to determine its current financial status.

AFP investigators were able to show Execom what intrusion had been made, but for a one-week period things were quite hectic at Execom. The company estimated that it cost US$20,000 to repair the damage caused by 'Phoenix'.

'Phoenix' also penetrated NASA networks in Virginia to the extent that it voluntarily disconnected its networks form external commu-

nication links for 24 hours in an attempt to re-establish the integrity of its systems.

Apart from the damage and security concerns raised in this case one particular facet was considered to be very serious given the future ramifications of this single incident. During his activities "Phoenix" illegally obtained a copy of *Zardoz*. This document listed the known security weakness of computer systems using the UNIX operating system. The editor of this document stated that up to 90 per cent of the computer systems connected to Internet would be vulnerable to intrusions if this document was released to hackers. Internet is the name given to a collection of computer systems which share a interlinked communications network. There are more than 2 million private, commercial, military, educational and government network nodes attached to Internet. Australia accounts for approximately 70,000 of these links. Unfortunately, the AFP has found copies of *Zardoz* in the possession of other computer hackers.

This matter has recently been finalised in court. The presiding judge, Justice Smith, stated that he considered computer crime to be serious and that these crimes have an infinite potential for damage. When asked what he meant by this he said: "There is no limit to what they can do". The sentences handed down by the court in this case were:

**Nahshon Even-Chaim alias 'Phoenix'.**

- Sentenced to 12 months imprisonment on each of four charges, all to be served concurrent and suspended for a period of 12 months.
- Sentenced to nine months imprisonment on each of seven charges, all to be served concurrent and suspended for a period of nine months.
- Convicted on a further three charges and placed on Community Based Order. He was further directed to serve the maximum period available under Commonwealth legislation of 500 hours of unpaid community work.

**Richard Martin Jones alias 'Electron':**

- Sentenced to six months imprisonment on each three charges, all to be served concurrent and suspended for six months.
- Convicted on a further 11 charges and placed on Community Based Order. He was further directed to perform a period of 300 hours of unpaid community work.
- He was further directed to submit himself for psychological or psychiatric assessment and treatment as may be directed.

**David John Woodcock alias 'Nom':**

- Sentenced to six months imprisonment on one charge - suspended for six months.
- Convicted on another charge and placed on Community Based Order. He was further directed to perform 200 hours of unpaid community work.

Operation Dabble was an important and successful investigation which cannot be gauged by the sentences handed down by the courts. The primary goal was first and foremost to stop the offenders from continuing to access US Military Networks. The AFP achieved this, but if The Realm's activities not been stopped, the possibility existed that they may well have been continuing with their criminal acts today. If this were the case, the political ramifications for Australia can only be imagined.

Operation Dabble was the first case of this kind in Australia and helped establish three important points:

- it removed the no-victim 'myth' from computer crimes and provided substantive facts on the potential threats to our country as well as to other countries from this type of crime;
- it showed that Australia has effective Commonwealth computer crime legislation;

and most importantly

- it demonstrated that the AFP has the resources and skills to successfully investigate complex national and international crimes.

The AFP's success in combating this type of crime cannot be easily measured, but it is clear that society cannot afford to ignore this type of criminal activity. If it does then the capacity to protect key elements of modern Australia may be lost. Sensitive information may not remain secure, and communication systems may be vulnerable to attack.

Increasingly, the effects of computer crime is being experienced internationally. Operation Dabble is not the only major computer crime investigation conducted by the AFP to date, but it was the first and, if nothing else, it heralded a serious attack on the security of what much of what modern society takes for granted.

## Computer hacking is not child's play

- In March 1991 a hacker disrupted a weather satellite terminating the capacity to predict weather patterns in parts of Europe for approximately one week. During this period a severe storm hit the Bay of Biscay. There were no weather warnings provided to shipping in this area.

  A ship sank as a result of damage inflicted by the storm. It can only be postulated as to whether this ship would have sunk had it been warned of the storm.

- An unknown hacker changed the research results that Turin University had been conducting into AIDS. There were no viable backups of this data. In effect all the research was lost because the research data cannot be validated. Who can measure the cost this single incident will have on AIDS research.

- In Luxembourg a hospital's network was severely damaged during a 'hack'. The results of this single event can be measured through the impact this event had on a 10 -year-old boy. He was suffering from cancer and required an operation. This operation was delayed for six days because of the hospital's network had to be rebuilt.