COMPUTER HACKERS: JUVENILE DELINQUENTS OR INTERNATIONAL SABOTEURS?

Suelette Dreyfus
Author

Paper presented at the conference: Internet Crime
held in Melbourne, 16-17 February 1998, by the Australian Institute of Criminology
INTRODUCTION

I’m here to talk about hackers and particularly hackers in Australia. In broad terms, the topics I will cover today are:

- What is a ‘hacker’?
- How widespread is hacking?
- What are the key hacking cases in Australia?
- What motivates a hacker?
- What are the common themes among elite hackers?

WHAT IS A HACKER?

The original definition could best be given as: anyone who ‘breaks open’ code and manipulates it in a clever or original, but not necessarily illegal, fashion. However a more recent definition would be: anyone who breaks into a computer without authorisation. Breakers are people who ‘hack’ the telephone system illegally.

This is separate and distinct from fraudsters, for example, who commit credit card or other fraud, some of which may be conducted over computer networks.

Hackers would also generally not consider, for example, a disgruntled employee who breaks into his or her company’s computer in order to ‘get even’ to be a ‘hacker’ per se.

Hackers use handles - on-line nick names - to disguise their identities and to present a particular image of themselves.

There is a distinct hierarchy in the hacking community, with elite (experienced) hackers at one end, and ‘Script Kiddies’ or ‘Script Weenies’, inexperienced hackers who use automated programs to break into computers, at the other.

Top tier hackers usually have a sort of ‘code of honour’. This code tends to make them ‘look-see’ hackers, that is, hackers who ‘look’ to see rather than to sell or to do purposeful damage. In particular, this code of honour means:

- They ‘look but don’t touch’ and try not to do damage.
- They do not, for example, delete data files. But they might delete or alter logs, to cover their tracks.
- They might copy data in order to study it themselves.
- They would not sell or otherwise profit financially from either the data or their illegal hacking.

Australian hackers have been a part of the world-wide hacking scene since the mid to late 1980s. Between 1989 and 1996, some of the world’s best hackers were Australian.

The Australian hacking community may have strong links to hackers overseas, but the experience of Australian hackers has differed from those in the US, most significantly in that they have tended to receive non-custodial sentences.
HOW WIDESPREAD IS HACKING?

In two words: reasonably widespread. It is certainly more widespread than the number of actual cases reported each year.

However, it is probably less widespread than described by some ‘hype merchants’ in computer security consultancies and other organisations. Yet the number of attacks is rising as the Internet continues to grow. One American security company, WheelGroup, conducted a survey of security incidents based on 556,464 security alarms from May to September 1997, from its customer base. Important elements of this survey were:

- Unlike many security incident surveys, this survey segmented the attacks. Some were classified as Serious Confirmed Attacks, such as Syn flooding, pings of death, cgi-bin web exploitation, and sendmail exploitation. Others were classified as probes, such as port sweeps, ping sweeps and high zone transfers, which might or might not be malicious.

- Although flawed in some ways, the survey findings were interesting and indicative if not exact. It found that:
  - Serious attacks occur 0.5 to 5.0 times per month per customer of the security company
  - 48% of attacks originate from ISPs as opposed to independently registered addresses
  - 39% of all attacks detected originated outside the U.S.
  - ‘Copy-cat’ attacks, usually by Script Kiddies, were on the rise

The survey effectively traced the last 'hop' of a hacker in an attack. This meant for example, that if a Swedish hacker broke into a French system and then launched an attack on a US system, the attack was registered as coming from France, not Sweden.

Few surveys, if any in this area, are completely accurate, however, they provide a useful indication of trends.

A TIMELINE OF KEY AUSTRALIAN HACKING CASES

Another method of viewing trends is to develop time lines of actually hacking cases. This is one method used in the book, ‘Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier’. Important events in the history of Australian hacking cases include:

- 1989 - The WANK Worm that ate NASA - believed to be created by Australians. Case never solved.
- 1989 - Australian Commonwealth computer crimes legislation passed
- 1993 - ‘The Realm’ case - Three hackers convicted in the first major hacking case in Australia
- 1994 - ‘Anthrax, a phreaker and hacker, is convicted. Interestingly, he is from a country area, unlike most convicted hackers which are from cities.
- 1996 - (Dec.) - The last of the three ‘International Subversives’ hackers is convicted.
- 1996 - (Dec.) - The Crawler, aged 21, pleads guilty to charges in a Brisbane court.
The details of these cases, and some others, which are roughly in chronological order, follow.

**The WANK Worm**

The WANK worm is known by its acronym, standing for the ‘Worms Against Nuclear Killers’. The worm wreaked havoc on NASA’s and the US Department of Energy’s computer networks. The worm launched thousands of attacks. Although numbers of successful penetrations were sketchy, probably 250 machines were successfully invaded, according to an internal NASA estimate. The incident was not widely reported, largely because NASA was very sensitive about it and because the attack coincided with anti-nuclear protests regarding the launch of the plutonium-powered Galileo space probe.

What is interesting is that this appears to be the world’s first politically motivated worm - in that it was bearing an antinuclear message. It was also the second major worm in the history of worldwide computer networks.

The worm was developed on a machine France, but logs showed the creator had come from Australia. The worm had a process name: OILZ. The word meant nothing to the American investigators at the time, but is almost certainly a reference to the Australian music band Midnight Oil.

There was a second, more subtle, indication that the worm was an Australian creation. The worm’s anti-nuclear banner had a saying:

> ‘You talk of time of peace for all and then prepare for war’

The anti-military quotation which appeared on the WANK worm banner was in fact from a Midnight Oil song, called “Blossom of Blood” on the “Species Deceases” CD.

**The Realm**

This tale is about the first major hacking legal case in Australia. ‘The Realm’, a Melbourne hacking board, involved three hackers: Phoenix, Nom and Electron.

They hacked Eugene Spafford’s and Cliff Stoll’s machines. They had strong ties with both American, British and German hackers, particularly with Erik Bloodaxe, the British 8LGM hackers and the German hacker Pengo. They were incredibly active. They made the front page of The New York Times.

Indeed, Australian hackers were so active in this period that American investigators believed initially that they were chasing a worm or virus because so many sites were being hit. It came as some surprise that in fact it was all being done by just a few people.

The hackers were aged between 18 and 22 at the time of the offences, and were later convicted of breaking into NASA, CSIRO, L. Livermore National Laboratory and other sites. All three received suspended sentences of 6-12 months, community services orders of 200-500 hours, and good behaviour bonds.

Electron experienced periods of serious mental illness from 1991 onwards, and spent time receiving extensive psychiatric support inside hospital. He is now fully recovered.
**Anthrax**

This case refers to the Australian fundamentalist Islamic hacker “Anthrax” who obtained control over telephone exchanges of dozens of military sites. Anthrax was so obsessed with hacking that he described hacking for up to 40 hours without a break, stopping only to eat or pray. As a religious Muslim, he had to pray five times a day. So he would hack all night and then as dawn approached, he would be in some interesting system but he would have to pray. He used to press ‘control S’ - pause his hacking, roll out his prayer mat, pray briefly, then press ‘control Q’, and return to his hacking.

He was convicted in 1994. The DPP (the prosecutor) had asked for 1500 hours of community service if he couldn’t arrange a prison sentence, but this proposal was rejected by the judge. The final sentence included 200 hours community service and restitution payment of more than $6,000 to two Canadian phones companies.

**The “International Subversives”**

The International Subversives were an Australian hacker group which conducted the largest ever security breach in the internal network of one of Canada’s biggest telecommunications companies - NorTel (Northern Telecom). The security incident report used in court case was 675 pages long.

They hacked a US military machine, at the US Department of Defence’s Network Information Center (NIC). NIC provided a crucial service at the time: it assigned domain names for entire Internet. Thus their control over it gave them enormous power.

The IS Hackers were particularly good at the art of piecing together information from assorted emails held by third parties. They used this method to spying on the police who were investigating them at the time.

In December 1996, the last of the three IS hackers was sentenced in court. Like the Realm hackers, none of the IS hackers received non-suspended custodial sentences. Two IS hackers were ordered to pay reparations for $2100, had convictions recorded, and received good behaviour bonds. The third received no recorded conviction, and a good behaviour bond largely because his history psychiatric illness.

All three had suffered breakdowns or periods of mental illnesses after the raids by police at their homes. One of them spent a brief time inside a psychiatric hospital, and another was on medication for an extended period. They are all also fully recovered.

**The 8LGM Case**

The first is the “8LGM” case in Britain - the first major non-employee hacking court case under the 1990 Computer Misuse Act. Again, it involved three hackers: Pad, Gandalf and Wandii. The hacking group was named after a music band called “The Eight-Legged Groove Machine”.

They were charged with conspiracy to commit a crime, even though they had never met each other.
One hacker, ‘Pad’, was also charged with causing damage to a computer. The police initially claimed the hacker had caused a quarter of a million pounds of damage. The true value of the damage was less than 15,000 pounds - a fact later conceded by the prosecution.

Two hackers received 6 month prison sentences. They served 3 months, where they shared a cell.

The youngest hacker, ‘Wandii’, pleaded not guilty and took his case to full trial - one of the few examples of a full trial hacking case in Britain or Australia. A professor, the head of the National Addiction Centre, gave crucial evidence. He had assessed Wandii, and essentially found him to be obsessed with the intellectual thrill of hacking. He compared the obsession to that of a compulsive gambler. The jury acquitted Wandii in less than 90 minutes.

**The Rome Labs Case**

This refers to the 1997 The Rome Lab Case in which two UK-based hackers, ‘Datastream Cowboy’ and ‘Kuji’, attacked large numbers of US military and other sites in early 1994. ‘Datastream Cowboy’ was a minor at the time of the incidents. Kuji was about aged 21. The attacked sites included the US Air Force’s Rome Laboratory in New York state.

After a prolonged investigation by officers from US Air Force and the Metropolitan Police CCU (UK), the hackers were charged. Datastream Cowboy eventually pleaded guilty to 12 minor charges in March 1997. He was fined 1,200 pounds for offences related to unauthorised access of computers (Computer Misuse Act 1990). In November 1997, the prosecution decided not to proceed with the case against Kuji. It is notable that Kuji had links to an Australian underground bulletin board.

This case is interesting as it provides a reality check on the hype surrounding claims of ‘information warfare’ and ‘info warriors’. The US military and other parts of the US government used these two hackers as evidence of the dangers posed by ‘international terrorists’ using the worldwide computer networks to attack the United States. The hackers were used as examples in reports by the US Air Force, the Government Accounting Office, the Pentagon's Defense Science Board report on information warfare, and the recent Marsh Commission.

A US Government Accounting Office report stated: “Air Force officials told us that at least one of the hackers [of Rome Labs] may have been working for a foreign country interested in obtaining military research data or areas in which the Air Force was conducting advanced research”.

In fact, ‘Kuji’ and ‘Datastream Cowboy’ were just bedroom hackers, not the professional espionage menace presented by the US government. They were not working as foreign spies.

One of the hackers admitted that his main interest was to find if the US government’s ‘Area 51’ in Nevada, which has achieved popular notoriety amongst X-Files fans, was in fact a secret hangar for capture alien spacecraft.

**WHAT MOTIVATES A HACKER?**

What motivates top hackers? Each hacker is different of course, however these direct quotes from hackers themselves provides some insight:

- ‘It’s not for personal gain.’ - Electron
- ‘The kick of getting into a system. It’s the ego boost from doing something well where other people try and fail. Once you are in, you very often get bored and may never call back. Because once you’ve gotten in, it’s a challenge over.’ - Electron
- ‘Once you get into the first system, it’s like, you get into the next one, and the next one, and the next one . . . like forbidden fruit.’ - Anthrax
- ‘To own the system’ - Anthrax
- ‘[At first it was] possibly the sheer lust for power or [the desire] to explore an intricate piece of technology. [Now] my first and foremost motivation is to learn.’ - SKiMo
- ‘Possibly it is just the satisfaction of knowing that what I learn is proprietary - it is inside knowledge.’ - SKiMo
- ‘I’m just addicted. I wish I wasn’t.’ - Wandii. (This statement was repeated 12 times in his police interview.)
- ‘It ain’t a malicious thing. It’s a challenge - the thrill of the chase. Sometimes I think I hack just to be able to say that I do something, like its a fad or something.’ - Case

While it is difficult to pinpoint a 'profile of hacker' it is possible to detail common themes among types of hackers, in this case among elite hackers. These themes were observed as part of the two years of research for the book ‘Underground,’ including a number of interviews with a number of hacker themselves. These include:

- In general, they are very bright or gifted.
- Their ages at the time of the most frantic and sophisticated hacking were usually between 16 and 24.
- They all admitted that they never quite fit at school or university. This might say more about the education system than the individuals themselves. In almost all cases, they had moved far beyond anything that school or university could teach them about computers in particular fields. Often they described feeling alienated by teachers, whom, it would appear, were ill-equipped to deal with gifted children.

- Most were also introverted, anti-social perhaps even awkward. They usually came from less than picture perfect family backgrounds. Their families were often dysfunctional, in some cases with one parent missing, through divorce or death. In Electron's case, both parents died of cancer. Prime Suspect's father died of cancer. In Mendax and Phoenix's case, the parents had both divorced. In Anthrax' case, his father was physically abusive.

- An anti-establishment view is a key factor for the top hackers. They want to rebel against symbols of authority, such as banks, government agencies and what President Eisenhower called the ‘Military Industrial Complex.’

- They would often describe themselves as being addicted to or obsessed with being on-line, often spending up to 40 straight hours hacking.

- They said they were often driven by the adrenalin rush of being somewhere they were not supposed to be.

- More experienced hackers visit a system numerous times, while less experienced hackers tend to use a system as a one-hit adventure. One hacker of mid-level skill estimated that he never returns to 75 per cent of the systems he hacks, and he only returns to 5 per cent of systems more than 10 times.
- They have tended to experience periods of mental illness or emotional breakdown, particularly immediately after being raided by police. This would seem to be related to being denied access to their gear (computers, modems etc). In some cases, they subsequently moved into drug addiction, perhaps substituting drugs for hacking. This tended to be followed by some sort of mental or emotional breakdown.

- They tend to ‘outgrow’ hacking. Several years after being charged by police, they say they no longer are involved in hacking. While certainly, it is possible they are simply ‘saying’ this to protect themselves, other statements from them appear to be consistent with actually ‘outgrowing hacking’. In particular, they have tended to develop more well-rounded lives, establishing relationships, starting jobs, developing hobbies. For example, several hackers developed their interest in music by forming bands. A number said they now consider computers a ‘way to make a living’ not to have ‘fun’ per se. Interestingly, while many do not feel what they did was ‘’, they do express regret at the stress they caused to the system administrators of the systems they hacked.

This paper does not suggest that all hackers are benign - clearly that is not the case. Some hackers are malicious, most are a nuisance. Leaving a computer system which is not secured attached to any network - particularly the Internet - carries a degree of risk. Clearly, prevention is better than cure. However, at this time, it appears that most hackers, particularly those in the elite category, are not the international saboteurs or professional information warriors presented so frequently in the media. Rather, as these cases illustrate, they tend to be bedroom hackers with a set of motivations closer to teenage graffiti artists than spies involved in corporate or international espionage. Importantly, based on anecdotal evidence, there appears to be a link between hacking, particularly at the highly skilled end of the spectrum, and mental illness, addiction or obsession, and this link deserves more in-depth study. Finally, it is noteworthy that, in most of the cases studied for this paper, when the hackers received proper support and treatment, they were able to move beyond hacking and to become productive members of society.