Australian Government
Australian Institute of Criminology

AUSTRALIAN HIGH TECH CRIME CENTRE

HIGH TECH CRIME BRIEF

# Hacking motives

2005

06

## Nuisance or crime?

Hacking has multiple meanings and is commonly used to refer to forms of trespass against a computer belonging to another. This brief examines the motives for hacking, in the sense of trespassing against another person's computer. However, this does not match the general criminal definition of hacking-type offences. An intention to commit a serious offence, or to cause harm or inconvenience, lies at the heart of the definition of the more serious computer offences under Australian laws modelled on the *Cybercrime Act 2001* (Cwlth). Accessing data alone is an offence where there is an intent to commit a serious offence. The modification or impairment of data is an offence if accompanied by an intention to cause (or recklessness as to causing) harm or inconvenience. Other offences under this model are based on breach of access restrictions in relation to data. Only in Tasmania is the law framed without reference either to the intention of the hacker, or to access restrictions on the computer being hacked.

### Criminal intent

The requirement in Australian anti-hacking laws for an intent to commit a serious offence, or cause harm or inconvenience, creates a high barrier for the prosecution to prove that a specific hacking incident is criminal. On the other hand, the category of recklessness as to harm or inconvenience caused by hacking invokes a standard of reasonably foreseeable consequences. Those who hack should be aware that, whatever their own intention, the convergence of technology and criminal activity heightens the risk that any hacking activity could become the platform for serious damage over the internet. Some hackers clearly intend to cause serious damage; for others, how far the law extends liability for hacking activity that is taken up and used maliciously by others remains to be seen.

## 2004 Victim survey

The 2004 AusCERT computer crime and security survey asked respondents what they thought was the motive for any hacking attack experienced in the survey period. Fifty-one per cent of respondents attributed at least one attack to indiscriminate action. Such attacks occurred simply because they were connected to the internet, making them vulnerable to hackers anywhere, or to automated hacking tools. Forty-one per cent thought that hackers were utilising system resources for personal use. The respondents attributed different motives for various hacking attacks: to demonstrate skill (40%), malicious damage (34%), to anonymise further attacks (26%), financial gain (18%), unknown reason (18%), personal grievance (14%), political hacktivism (9%) and competitor commercial attack (4%).

## Motives

The motives for hacking are varied and offenders form a heterogenous group. Grabosky and Smith (1998: 52–53) catalogue possible motives of hackers. They define hacking as unauthorised access to computer systems (hindering the operation or performance of a system or damaging its contents being referred to as vandalism). As they point out, the reasons given by hackers for their actions are likely to be self-serving and should therefore be treated with scepticism. In order to make sense then of the actions of hackers and begin to evaluate their explanations for hacking we must consider the full range of motives that underlie behaviour of this type. These authors cite a number of explanations for hacking that can be divided between those that are more likely and those that are less likely to indicate an intention to commit a serious offence, or to cause harm or inconvenience in accordance with Australian law based on the *Cybercrime Act 2001* (Cwlth) model.

The Act's test of intention for criminal hacking is less readily inferred where the motive is:

- monetary gain;
- intellectual challenge;
- power;
- self-expression and peer recognition (often focusing on military and other secure targets); and
- youth, frivolity, mischief or curiosity (unleashing unknown consequences).

The test of intention for criminal hacking is more readily inferred where the motive is:

- vengeance and vindictiveness;
- attacking the 'system';
- terrorism;
- self-justification through minimisation of harm (often ignoring remedial costs, inconvenience, collateral damage and resource waste); and
- 'testing' computer security.

Kilger et al. (2004) summarise the motivations of hackers (in a general sense) using the acronym MEECES, which is a play on the FBI acronym of MICE (money, ideology, compromise and ego) representing the motives for the commission of espionage offences. MEECES stands for money, entertainment, ego, cause, entrance to social groups and status. While this provides an easy to remember outline of the motivations of hackers, the analysis is constrained to fit the acronym. For example, intellectual curiosity is not given the prominence it should be. Combining the work of Kilger and Grabosky and Smith provides six generic headings that describe the various motivations for hacking. While the motives of money, entertainment, ego, entrance to social groups and justification may be less likely to involve the required specific intent, criminal liability may arise on the basis of recklessness regarding any harm or inconvenience caused. Cause or malice is the final motive in this list and is more inherently criminal. It encompasses the ideas of vengeance, 'attacking the system' and terrorism.

### Money

The ways in which money can be raised include: transferring funds electronically (credit card skimming, ATM card and password scams), stealing valuable data, stealing valuable services or capacity (such as for communications or data storage), stealing intellectual property (piracy), extortion, diversion to premium telephone services, fraud and marketing schemes (client lists, email lists, free, linked and subscription site payments). There is increasing evidence of organised criminal activity involving, for example, persons in Russia, Romania and Ukraine.

There has been a convergence of hacking activity performed for monetary gain:

- in July 2004, employees of an IT service company contracted by the Commonwealth Bank, were alleged to have used bank computing capacity to download, save and reproduce pirated adult pornography;
- hackers sell email lists to spammers who create backdoors using Trojan horses

– infected computers may then be made available as part of a 'bot army' to launch denial of service attacks enabling extortion (online betting services); and

- in the US, an employee of AOL has been charged with stealing the email subscriber list and selling it to a spammer who then sold it to others (The smoking gun 2004).

### Entertainment: youthful frivolity, mischief or curiosity

In this category are those who hack for personal pleasure. This form of diversion may often be an offshoot of involvement in gaming and code writing. Grabosky and Smith (1998) cite the launching of the Morris worm, which partially disabled the internet, as an example of the result of curiosity leading to unexpected consequences.

### Ego: intellectual challenge

This category includes those who hack to meet an intellectual challenge. These persons are not necessarily interested in any outside recognition. For hackers with this motivation there is a special challenge to be met in hacking into secure or high profile sites. Simon Vallor, who wrote the ResediB, Admirer and Gokar viruses, claimed he did so 'to see whether I could do it' (Leyden 2003). Vallor was convicted under the *Computer Offences Act* (UK) and sentenced to two years imprisonment.

The intellectual challenge is often the motivation of those who create viruses or worms that work on a vulnerability to create a new exploit. In so doing, these hackers provide a platform for others to make malicious use of the exploit. An example is the creation of backdoors in systems that can then be used by spammers and others such as with the Bagle.B worm (Sydney morning herald 2004).

### Entrance to social groups/status

The stereotypical image of the hacker as a lonely computer geek belies the fact that hackers constitute a well developed but heterogenous community. Some hackers may be motivated by this sense of community obtained through sharing their experiences with others and may hack computers simply to stay in touch with the hacking community. Online communities can be extremely absorbing and not only provide peer recognition, but also the tools to hack through the sharing of knowledge, skills, techniques and technology. Sometimes there is a division among subgroups of hackers and hacking becomes, in itself, a way for these groups to express their rivalry and to compete for supremacy. This has been seen with messages embedded in the code of worms (Kotadia 2004b). The case of David Smith is illustrative of the use of hacking to gain enhanced status in mainstream society. Smith wrote the Melissa worm and later submitted a version for a college thesis (Fuquay 2004). Adrian Lamo broke into the computer systems of major corporations so that he could then offer to fix them for free (Hulme 2003).

### Justifications: minimising harm, testing computer security, claim of right, vigilantes

Hackers may operate out of a sense of self-justification. They may do this by downplaying the damage caused or their own awareness of the potential for damage to be caused. Others may argue that they were testing a network or computer. A case of this type involved students accessing privileged information in the computer network of Oxford University and then writing up the results in the student magazine. Other cases may involve genuine disputes over ownership of data particularly where a person is moving from one business to another. There are also vigilantes who take it upon themselves to investigate the illegal activities of others. In one example a hacker in Turkey provided information to law enforcement and this was then used to obtain a warrant to search the computer in the United States of a person accessing child pornography (*US v Steiger* 2003 WL 115261 (11th Cir. 2003); *US v Jarrett* 338 F. 3d 339 (Va., 2003)).

### Cause/malice: attacking the system, vengeance and vindictiveness, power, terrorism

Hackers may be motivated to commit widely distributed attacks on large targets such as have been experienced by Microsoft involving the MSBlast worm which carried an embedded message critical of Microsoft's founder Bill Gates (Kotadia 2004a). Another widely distributed attack targeted the SCO corporation, following its claim to part of the source code for Linux operating software (Moore & Shannon 2003).

Some hackers are motivated by individual grievances leading to attacks on individuals or companies. An example of an individualised attack that lead to widespread harm in the physical world was the hacking of the sewage treatment system in Queensland, which caused raw sewage to be pumped into waterways. The offender was convicted and sentenced to two years imprisonment (Smith et al. 2004).

It is increasingly being recognised that web-based illegal activity may be used to finance terrorism.While computer hacking may in the future be used directly to further terrorist aims, this does not appear to have occurred to date. Hacking has the capacity to cause damage, or aggravate damage from other forms of attack. Items that are critical to the national information infrastructure or key utilities involving energy, communication, health and hazardous materials provide obvious targets for malicious hacking.

## Conclusion

Importantly, hacking remains a contested concept incorporating, for example, the inherently contradictory values of the so-called 'white hat' and 'black hat' communities, which simplistically equate to 'good' and 'bad' hackers. Sometimes malicious hacking is separately labelled as 'cracking' in order to differentiate it from benign or good hacking. Ultimately, these labels give way to the legal tests laid out for hacking offences, which include recklessness as to the harm or inconvenience that a hacker may cause, thus potentially capturing the well-meaning hacker. It is important to understand the many possible motives for hacking in a general sense because issues of intent and recklessness are at the heart of criminal liability. With this knowledge we can better detect and deal with offending behaviour.

Contact
Australian Institute of Criminology
GPO Box 2944 Canberra ACT 2601
Phone: 02 6260 9200 Fax: 02 6260 9201
Web: www.aic.gov.au

Project no. 0074 ISSN 1832-3413



The Australian High Tech Crime Centre funded this research.

## Further reading

AusCERT 2004. *Computer crime & security survey.* Brisbane: AUSCERT

Fuquay J 2004. Getting caught in the brag net of cybercrime fight. *Canberra times* 9 February

Grabosky P & Smith R 1998. *Crime in the digital age.* Sydney: Federation Press

Hulme G 2003. Flurry of arrests made in cybercrime cases. *Information week* 15 September

Kilger M, Arkin O & Stutzman J 2004. Profiling. In *The honeynet project know your enemy: learning about security threats* (second edition). Boston: Addison Wesley. http://www.honeynet.org/book/Chp16.pdf

Kotadia M 2004a. New version of Mydoom to launch new attack. *Sydney morning herald* 10 February

Kotadia M 2004b. Worm authors talk trash. *ZDNet UK* 4 March. http://www.zdnet.com.au/news/security/0,200006174 4,391161418,00.htm

Leyden J 2003. Welsh virus writer Vallor jailed for two years. *The register* 21 January. http://www.theregister. co.uk/2003/01/21/welsh_virus_writer_vallor_jailed/

Moore D & Shannon C 2003. *SCO offline from denial of service attack.* CADIA. http://www.caida.org/analysis/security/ sco-dos/

Smith RG, Grabosky PN & Urbas GF 2004. *Cyber criminals on trial*. Cambridge: Cambridge University Press

Sydney morning herald 2004. New worm appears, spreading rapidly. *Sydney morning herald* 18 February

The smoking gun 2004. Pair nailed in AOL spam scheme. *The smoking gun* 23 June. http://thesmokinggun.com/ archive/0623042aol1.html