Australian Government
Australian Institute of Criminology

AUSTRALIAN HIGH TECH CRIME CENTRE

no. 11 ▪ 2006 HIGH TECH CRIME BRIEF

More malware – adware, spyware, spam and spim

Potentially damaging forms of malicious software (malware) such as viruses, worms and Trojans infect large numbers of computers around the world and interfere with internet-based telecommunications (High Tech Crime Brief no.10). Other forms of intrusive program, not necessarily as damaging as, but potentially hiding these more virulent types of malware, circulate as adware, spyware, spam and spim. Even where these forms of malware are free from code that can damage or interfere with computer functions, they can still be misused to promote unwanted products, disseminate offensive content, or provide unauthorised access to personal and financial information.

Adware and spyware

Adware is a kind of software that usually causes 'pop-up' or banner advertisements to appear on the computer's screen when a user clicks on a link, accesses a website or initiates some other function. The purpose behind most adware is commercial – to recover all or some of the cost of providing free or low-cost software or maintaining websites – but it is usually regarded as irritating to users when it appears without their consent or because it is hard to remove once installed on a computer. In some cases, the adware promotes adult products or pornographic websites, and is therefore offensive to many users.

Spyware is sometimes incorporated into adware, but performs the additional function of surreptitiously monitoring details of computer usage and website activity, making this information available without the knowledge of the user. Some spyware installs programs known as 'key-loggers' to collect user identification, passwords, personal and financial information, and email addresses, and send this to the originators or controllers of the spyware, or to third parties. It is therefore a significant enabler of credit card and other fraud, identity theft and related crimes. Less dramatically, spyware also allows advertisers to direct advertisements towards internet users based on their interests as indicated through web searching and website visits, and in some cases is used to redirect users through hijacking of hyperlinks to particular websites rather than commercial rivals' websites.

Spam and spim… and maybe spit?

Spam is the electronic equivalent of 'junk mail' which is unsolicited, usually sent in bulk transmissions of thousands or even millions of messages at a time, and significantly impedes the flow of legitimate internet traffic around the world. Spam is facilitated by the automated harvesting of email addresses from websites, email accounts and, to an increasingly significant extent, by spyware. Some spam advertises harmless though usually unwanted products such as personal finance or consumer goods, but some offers adult products and pornography. Because this type of content is unsolicited and is often offensive, internet regulators and legislators have begun to place controls on spam activity, such as the *Spam Act 2003 (Cth)*, in force from 10 April 2004, which makes it an offence, punishable by civil penalties such as large fines, to send bulk unsolicited email in Australia or to Australian recipients. Some other countries have enacted criminal offences to counteract spamming. In the United States, several prosecutions have resulted in convictions under the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, which came into effect on 1 January 2004.

SPAM CASES In one of the first cases to be brought under the *Spam Act 2003 (Cth)*, the Australian Communications and Media Authority (ACMA) obtained declaratory orders against a business that sent over 200 million unsolicited commercial electronic messages to email addresses that had allegedly been harvested using automated software: *Australian Communications and Media Authority v Clarity1 Pty Ltd* [2006] FCA 410 (13 April 2006). Civil penalties are yet to be imposed.

In the United States, within a month of the CAN-SPAM Act's commencement in 2004, the Federal Trade Commission had identified two large-scale spammers from consumer complaints detailing massive numbers of unsolicited messages offering such products as 'diet patches'. Subsequent litigation resulted in settlements including prohibitions on further spamming activity. In one case, the defendant company was based in Australia, and was ordered to hand over more than US$2 million in illicit profits from spamming activities offering human growth hormone products (FTC Media release 20 Sept 2005).

Project no. 0074a

ISSN 1832-3413

The Australian High Tech Crime Centre funded this research.

CONTACT
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601

T: 02 6260 9200
F: 02 6260 9201
www.aic.gov.au

Spim is the version of spam that targets instant messaging (IM) services. It has increased in prevalence along with the use of mobile phones and other hand-held computer technologies to convey short messages rapidly. Some spim-related programs seek to get around protections used by instant messaging users, such as restricting contact to selected lists of known friends or acquaintances ('buddy lists'), by disguising the identity of message sources. For example, a spim sent to an unprotected mobile device may require the recipient to click on a link to remove the message, which then captures the user's identity details so that subsequent spims sent to that user's address list appear to be from that user. Thus, as with many forms of misuse of technology, there is a mix of intrusive methods, questionable content and opportunities for further criminality through identity crime.

Finally, *spit* is the version of spam that could affect internet telephony such as Voice over Internet Protocol (VoIP) services. It has not yet appeared 'in the wild' but patent applications for technology to counter this predicted risk have been filed and preventive solutions are entering the market (Schweitzer 2005). Hacking tools known as 'sniffers' are able to target VoIP vulnerabilities by capturing voice data over networks so that eavesdropping on conversations is made possible, with obvious risks to the confidentiality and security of information.

Infected spam and botnets

Spam in all its forms can be not only annoying but harmful when it involves hidden programs such as viruses/worms or other malware. For some time, the activities of spammers and virus/worm creators were relatively unconnected, but there has been a recent increase in the use of spam to drive malware dissemination and vice versa, with the result being a steady growth in infected spam messages. The added threat is that the recipient of spam not only receives unwanted email, but his or her computer then becomes (usually without this being known to the person) a vehicle for the dissemination of further spam/malware to other computers.

BOTNET CASES In the United States, a 20 year-old Californian has been convicted of dealing in botnets and offering these for sale to others for the purposes of sending bulk spam and launching denial of service attacks. This activity earned the dealer thousands of dollars from clients. The defendant pleaded guilty in January 2006 to computer fraud and spam offences, and was sentenced in May 2006 to 57 months in a Federal prison (US DOJ Media releases 23 Jan and 8 May 2006).

In a separate case, another 20 year-old Californian was indicted in February 2006 over the widespread use of botnets to install adware. It is alleged that he and others compromised large institutional computer networks at several universities in order to create a huge botnet, which resulted in damage including interference with the computerised systems in a Seattle hospital (US DOJ Media Release 18 Feb 2006).

Some spam-related malware utilises the address books found on personal computer email programs to send spam, while others operate by turning the host computer into a 'bot' that, along with thousands of other similarly infected computers in a 'botnet' created by the malware, can be instructed to send out massive quantities of spam. By utilising these methods, spammers have been able to flood the internet with so much bulk email that spam is now estimated to account for the major share of the world's internet traffic (Watts 2006).

Additionally, this linkage between spamming activity and botnet-dealing has provided motivation and funds for other uses of botnets such as destructive attacks on computers and networks. There are signs of emerging black markets in botnets and related skills and capabilities. In recent cases in the United States, several defendants have been convicted over the use of botnets to install adware without permission, send spam and launch denial of service attacks.

Spam and pornography

Reactions to spam vary according to its content. According to a recent United States-based assessment (Evett 2006), users are most annoyed at receiving unsolicited pornography (91%), followed by mortgage and loans offers (78%), investments (68%), real estate (61%) and software (41%). Concerns over pornographic spam, also known as sporn, arise largely because recipients of such messages may include children. The concern is magnified where particularly explicit or disturbing sexual imagery, which may include child pornography, confronts the receiver without his or her consent.

Known examples of sporn methodology include the use of spam or apparently innocuous emails that, when opened or even rolled over with a cursor, activate download programs that take over internet browsers and replace the recipient's homepage with a pornographic site or otherwise interfere with the computer's functions. Some porn-related malware installs automatic diallers onto computers, often connecting to high-priced services, or alters the start-up routines so that porn-related icons appear on the screen automatically. The use of email address 'spoofing' in such operations makes the source of emails harder to detect and also hides the connections to pornographic material. Many websites expose the visitor to such malware, including in some cases, non-pornographic websites.

Spim and pornography

With the increasing functionality and capacity of instant messaging, it is not surprising that spim has also become a vehicle for pornographic content dissemination. This can be either by means of content transmission directly, or by means of short messages inviting the recipient to click on a website link that contains pornographic content. In February 2005, a teenager in the United States became the first person ever charged with sending pornographic spim, allegedly involving 1.5 million messages. The defendant pleaded guilty to offences including extortion in March 2005 (US DOJ Media Release 22 Mar 2005).

FURTHER READING

All URLs were correct at 2 June 2006

Evett D 2006. 'Spam statistics 2006' *Spam Filter Review* http://spam-filter-review.toptenreviews.com/spam-statistics.html

Federal Trade Commission (FTC) http://www.ftc.gov

Schweitzer D 2005. 'Tired of Spam? Now there's Spim & Spit, too' *PC Today* vol. 3, no.5

United States Department of Justice (US DOJ) http://www.usdoj.gov

Watts P 2006. 'Don't make a meal out of spam' *IT Now (British Computer Society)* vol. 48, no. 1