Australian Government
Australian Institute of Criminology

AUSTRALIAN HIGH TECH CRIME CENTRE

no. 12 ▪ 2006 HIGH TECH CRIME BRIEF

High tech crime tools

High tech crime (HTC), also known as technology-enabled crime, makes use of information and communications technologies to infringe criminal laws. A range of methodologies is used, often employing tools which enable or enhance the commission of the offences in question. Online tools are those digital goods or services that can be obtained from the internet. They can be categorised as follows.

Illegitimate technologies

Some of the commonly seen programs that have no legitimate purpose and are used to commit HTC include bot and malware programs.

Bot programs, which operate automatically as agents for a user or another program, are surreptitiously forwarded to victims by a number of means. Upon successful installation, they can be used as remote attack tools or form part of a botnet to launch distributed denial of service (DDoS) attacks or to disseminate spam or malware. In March 2006, the AHTCC charged a Melbourne man with botnet-related activities and this case is due for a committal hearing in December 2006 (AHTCC 2006).

Malware programs are designed to penetrate computer systems without the owner's knowledge, often with the intention of causing damage. One common method of dissemination is via disguised email. The recent Dumaru worm, for example, disguises itself as a security patch from Microsoft, and installs an internet relay chat (IRC) trojan onto the infected machine once the victim executes the patch. Other malware programs include:

- Ransom ware – as recently as April 2006, several cases of cybercriminals using Arhiveus.A (aka MayAlert) to encrypt data on compromised computers for online ransom were reported – such activity is termed cryptovirology.
- Keylogging programs (keyloggers) are designed to monitor user activity including keystrokes. They can be used by cybercriminals to steal passwords or credit card details, which can then be used for malicious purposes such as identity/online fraud. Recent cases involving the use of keyloggers include an attempted theft from the Japanese bank Sumitomo Mitsui in London in March 2005.
- Rootkits are cloaking technologies usually employed by other malware programs to abuse compromised systems by hiding files, registry keys and other operating system objects from diagnostic, antivirus and security programs.

Legitimate computing technologies

Some tools leveraged for HTC are, in fact technologies designed to protect networks and computer systems or to copy and protect data for legitimate purposes. This is especially so when the distinction between accessing a system maliciously and network security analysis is at times blurred. A brief description of how legitimate computer security tools can be abused follows.

- Programs designed to protect copyright materials such as the extended copy protection (XCP) and the MediaMax CD-3 programs embedded in Sony BMG music CDs have been installed on computers when the CDs are played without obtaining consent from users. It has been discovered that the XCP program introduces system vulnerabilities enabling both programs to covertly transmit usage information back to the vendor and the music label. As a result, a number of lawsuits have been filed against Sony BMG leading the company to recall all affected CDs and release a software utility to remove the rootkit component (Halderman & Felten 2006). Shortly after the existence of both programs became public knowledge, a variety of malware exploiting the programs to avoid detection appeared (e.g. Stinx-E trojan).
- Steganographic programs that serve as information hiding tools when used in conjunction with cryptography can also be leveraged for secret communications by cybercriminals or terrorists to evade law enforcement scrutiny.
- Datamining programs allow users to obtain vast amounts of data from the internet. However, such programs can potentially be abused by cybercriminals to assume someone else's identity using information obtained from datamining.

Legitimate communications technologies

Increasingly, communications tools, never intended for criminal activities, are being or have the potential to be abused for HTC.

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

- Instant messaging (IM) and email programs remain popular due to their ability to enable real time chat and transmission of email messages. Such tools can, however, be leveraged for people-oriented HTC including social engineering, cyberstalking, internet scams or for the dissemination of viruses and worms. Cases of child grooming have also been reported as being facilitated by IM.
- Portable entertainment devices and USB storage devices can be abused as storage media for storing encrypted files or as vehicles for pirated songs and movies. As pointed out by Gordon and Willox (2006), such devices are also vulnerable to keyloggers and other forms of spyware.
- Digital cameras or camera phones can be used to facilitate HTC such as child pornography by covertly taking compromising pictures. They can also be used in connection with industrial espionage.
- Radio frequency identification device (RFID) chips are gaining popularity in a growing number of real world applications such as electronic passports and identification badges. Researchers from Vrije Universiteit Amsterdam and SRI International have suggested that RFID chips can be used to compromise computer systems by sending malicious data to vulnerable systems (Ortiz 2006). However, the likelihood of this happening in the real world is rather low at present (Mello 2006). Researchers from Germany have also demonstrated that e-passport RFID chips can be skimmed and cloned easily with inexpensive and easily obtainable equipment. They then speculated that the RFID tags embedded in US e-passports could potentially be used to identify passport holders from a distance – a form of short range clandestine tracking and scanning (Jay 2006). However, the US State Department has recently indicated that a Faraday cage to counter clandestine scanning and basic access control to counter skimming and eavesdropping of data will be included in the e-passport.
- Popular peer-to-peer (P2P) networks (e.g. Napster) and P2P services that use voice over internet protocol applications (e.g. Skype) can be abused to distribute copyright materials comprising pirated music and movies; distribute spam, viruses and worms; or launch attacks that cripple websites. Worms such as P2Load and the later variants of the Bagle worm have been known to proliferate via P2P applications. Studies have also indicated that sensitive/confidential corporate and personal data have been inadvertently made available to unauthorised personnel via P2P networks (Mathieson 2006).
- Internet sites are fertile grounds for learning how to commit HTC or terrorist acts, such as subverting computer systems and building homemade bombs. It is known that terrorists and cybercriminals have used search engines to search for keywords such as 'bomb making' or to search for sites detailing known system vulnerabilities that can be exploited.
- Support sites or blogs operated by cybercriminals might contain links to other networks such as networks of paedophiles and extremists, or act as a consolidated marketplace for pirated intellectual property. Such sites are often an effective way to reach an international audience, soliciting funding (for criminal activities), and recruiting new members, thus allowing cybercriminals to coordinate their activities and to distribute propaganda.
- Social networking sites, such as Friendster and Myspace, and chat rooms can be exploited for online sex predators. Recently, the US House of Representatives approved the *Deleting Online Predators Act 2006* that requires schools and libraries in the US to block access to such sites.

Knowledge based or hired help

Hacking organisations, cybergangs, and professional hackers are resources that can be employed by criminal organisations to carry out HTC. Examples include carrying out politically motivated hacking (hacktivism) and bringing down competitors' websites. Recent hacktivism incidents include defacing Danish websites by Islamic hackers protesting about controversial cartoons mocking the Prophet Muhammad. An example of hired help was an incident that took place in March 2005, where a 16-year old New Jersey hacker and his businessman hirer were arrested for launching DDoS attacks on competitors' websites.

Subscribing to security bulletins and scholarly publications allows cybercriminals to keep abreast of the latest security vulnerabilities and theoretical vulnerabilities. It is known that organisations generally do not patch their systems immediately when security vulnerabilities appear, so cybercriminals can take advantage of such vulnerabilities to compromise systems or to build viruses.

Countermeasures

Users in both the public and private sectors and software vendors are becoming more security conscious, which might explain the decline in the number of successful attacks on computer systems illustrated by recent statistics (CSI 2006).

Nonetheless, efforts to control the availability and use of HTC tools should be enhanced through technological solutions (e.g. datamining programs to aid in the grouping of similar programs written by hackers and tracing of their behaviour) and legislative efforts (e.g. the Council of Europe Convention on Cybercrime 2001). International collaboration between businesses and governments is also vital. This will help to combat criminal organisations that often take refuge in countries with limited or ineffective law enforcement resources.

FURTHER READING

All URLs were correct at 18 August 2006

AHTCC 2006. International internet investigation nets arrest. *Media release* 22 Mar

Computer Security Institute (CSI) 2006. *2006 CSI/FBI computer crime and security survey*. http://www.gocsi.com/

Gordon GR & Willox NA 2006. The ongoing critical threats created by identity fraud: an action plan. *Journal of economic crime management* 4(1): 1–15

Jay LJ 2006. Hacker cracks, clones RFID passport. *TechNewsWorld*, 8 Sept

Mathieson SA 2006. Peer-to-peer software exposes corporate data. *Infosecurity magazine* Jul/Aug: 5

Mello JP 2006. Is RFID a Pandora's box? *TechNewsWorld spotlight on security* Aug: 44

Halderman JA & Felten EW 2006. Lessons from the Sony CD DRM episode. *Proceedings of 15th USENIX Security Symposium*, 1–3 June 2006: 77–92

Ortiz S 2006. How secure is RFID? *IEEE computer* 39(7): 17–19