Australian Government
Australian Institute of Criminology

AUSTRALIAN HIGH TECH CRIME CENTRE

no. 13 ▪ 2006 HIGH TECH CRIME BRIEF

Acquiring high tech crime tools

High tech crime (HTC) tools are programs, devices or services that facilitate HTC. A brief overview of these tools is presented in *High tech crime brief* no. 12.

Locating online HTC tools

The proliferation of information and communications technologies (ICT) and connectivity of the internet opens the door to 24/7 fingertip access to most HTC tools. This is not surprising, considering the unsupervised and unregulated nature of the internet. The following illustrates some of the principal ways in which HTC tools can be acquired online. Some of these tools (e.g. virus creation kits, phishing kits, distributed denial of service (DDoS) kits, email bombers, botnet management kits) can be used with minimal levels of expertise.

Search engines and the internet – using search engines to search for keywords, such as 'hacking organisations' and 'network security analysis tools', is likely to return sites containing names of, or links to, hacking and network security organisations respectively.

Hacking/network security sites or blogs – hacking sites, particularly underground hacking sites and blogs, and some network security sites are rich sources for downloading tools that can be abused for malicious purposes, for example to gain clandestine entry into computer networks and systems.

- In one such network security site, the top 100 network security tools can be freely downloaded. These could potentially be abused for spying on other legitimate network users such as sniffing and cracking passwords (e.g. Cain and Abel), scanning the network environment for vulnerabilities for malicious exploitation (e.g. Nessus and Metasploit Framework), scanning for wireless network and decloaking hidden/non-beaconing networks (e.g. Kismet), and network auditing and penetration testing tools (e.g. Dsniff).
- Sites can be monitored for the latest news about system vulnerabilities including those discovered by members that have yet to be publicised. In several of these sites, step-by-step instructions on how to exploit known vulnerabilities are also provided. Cybercriminals can then take advantage of such knowledge to compromise systems, such as exploiting the security bug in the MS06-042 security patch released by Microsoft on 8 August 2006.

Peer-to-peer (P2P) networks – freely available P2P filesharing protocols create holes in corporate firewalls via an employee's desktop or laptop. Studies have indicated that sensitive/confidential corporate and personal data have thus been inadvertently made available to unauthorised personnel. Cybercriminals can crawl through P2P networks focusing on specific financial institutions/companies to find sensitive data – facilitating espionage, online fraud, identity theft, etc (Mathieson 2006: 5).

P2P networks such as Napster can also be abused to act as a consolidated marketplace for pirated intellectual property including software, movies and music, or child sexual abuse images. For example, in Operation Peer Pressure conducted by the FBI in 2003, child sexual abuse images were downloaded from offenders' computers via P2P networks.

Networking sites or blogs – many online HTC-oriented sites, such as hacking sites and blogs, can facilitate the creation of other support networks for HTC activities. In a study by Gerstenfeld, Grant and Chiang (2003), it was revealed that extremist and supremacist networking sites often contain external links to other sites of a similar nature and to materials or publications inciting extremist activities. Such sites are often an effective means of reaching an international audience, soliciting funding, and recruiting new members, allowing cybercriminals to coordinate their activities and to distribute propaganda. The recent report by NSTC (2006: 7) raises similar concerns.

Learning/updating technical skills

HTC is becoming more sophisticated and organised (Seger 2005), probably facilitated by ease of communication between like-minded individuals who know each other only online, and the internet making it easier to meet and plan activities, including crime. Another factor may be that profiles of cybercriminals significantly differ from those of traditional criminals. Recent studies by Kshetri (2006) and Jen, Chang and

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

Chou (2006) indicate that a sizeable percentage of cybercriminals in Russia and Taiwan belong to the educated Y generation group. Avi Rubin, professor of computer science at Johns Hopkins University, further suggested that hackers are now using academic resources more frequently and are more technically inclined than traditional criminals (McGraw 2006).

Institutes of higher education are places to learn the technical skills and education required for committing HTC. For example, the University of Abertay will be offering a Bachelor of Science (Hons) degree in ethical hacking and countermeasures (http://www.abertay.ac.uk/News/NewsPopup.cfm?NewsID=1038) teaching students the skills and techniques for defending systems against HTC.

Attending professionally run hacking conferences and training is also a way to learn and update technical skills. In one of the introductory training courses presented at the Blackhat USA 2006 conference, attendees with no previous hacking experience were taught hacking related skills such as coding and scripting, networking and internet technologies, basic methodologies, essential thinking skills, tools and current hacking techniques.

Although such training and courses are not all facilitators for crime, there is a possibility that some talented students may succumb to the temptation of illicit financial gain and abuse their knowledge to commit HTC. Terrorist groups are known to include engineers and computer scientists (NSTC 2006: 7). Moreover, there have been numerous reported cases of IT professionals committing HTC. For example, in September 2005, a former technology manager of a Silicon Valley based debt collection company in San Jose was convicted for placing a computer time bomb on the network that resulted in the corruption of over 50,000 debtors' records.

Purchasing HTC tools online

Although most HTC tools are freely available online, there are also some legitimate tools that can be purchased.

Recently, Swedish-based company RELAKKS (https://www.relakks.com/?lang=eng) set up a commercial darknet that allowed subscribers to establish secure encrypted communication. Darknets, loosely related to P2P networks, could potentially be abused by cybercriminals to distribute propaganda, images of child abuse, or copyrighted digital files in a secure manner to avoid the scrutiny of law enforcement agencies. Cybercriminals could use the obscurity feature to hide their identity. For example, they could use the RELAKKS system as an anonymiser since all traffic, regardless of its geographical location, will appear to be coming from Sweden. Moreover, RELAKKS assures its users that Swedish law enforcement agencies will not be able to obtain subscription information from RELAKKS unless there is a likelihood of imprisonment being imposed for the suspected offence (https://www.relakks.com/faq/security/).

Some of the HTC-oriented networking sites (e.g. Shadowcrew) have been known to traffic illicit wares (e.g. counterfeit credit cards, identification information and false documents, and stolen data using P2P networks) that could facilitate HTC such as identity theft. Other HTC tools such as botnets could also be purchased or rented from these network sites. The US Drug Enforcement Administration has recently closed down internet drug rings and rogue internet pharmacies offering controlled substances and pharmaceutical drugs for sale during their Cyber Chase operation.

Purchases of HTC tools can be paid through legitimate internet banking services (e.g. credit cards), pay per download websites, online payment systems, internet payment services and electronic cash. For example, it was reported that one bot seller in California received his payments for the rental and sale of bots through PayPal (http://www.schneier.com/blog/archives/2006/02/forprofit_botne.html).

An alternative method for cybercriminals to receive payments is via directed purchases. For example, in recent cryptovirology cases, victims were required to purchase pharmaceutical products from designated online pharmaceutical sites in order to obtain the password and decryption key required to unlock their data.

Prevention and control

Countering these risks requires collaborative efforts on the part of a wide range of government and private sector entities. These can occur at various levels:

- individual – ethical training, and perhaps, registration of IT students and professionals with computing professional bodies
- corporate – monitoring systems, enforcing corporate policies and disciplining rogue employees
- government – instituting more effective coordination with private sector organisations to identify illicit means of gaining access to tools online.

Specific strategies to minimise the risk of tools being misused include:

- proactive web scanning to detect and take down illegal sites and monitor hidden cyberthreats
- sharing information and intelligence among law enforcement agencies to detect and take down sites that trade illicit tools
- ensuring that complete forensic trails are established following a security breach (particularly tracing the digital money trail)
- designing tools to perform criminal network analysis identifying patterns of relationships and interactions (e.g. in extremist sites).

FURTHER READING

All URLs were correct at 18 August 2006

Gerstenfeld PB, Grant DR & Chiang C 2003. Hate online: a content analysis of extremist internet sites. *Analyses of social issues and public policy* 3(1): 29–44

Jen WY, Chang W & Chou S 2006. Cybercrime in Taiwan: an analysis of suspect records. Paper to Workshop on Intelligence and Security

Kshetri N 2006. The simple economics of cybercrimes. *IEEE security & privacy* 4(1): 33–39

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

McGraw G 2006. Interview: silver bullet speaks to Avi Rubin. *IEEE security & privacy* 4(3): 11–13

National Science and Technology Council (NSTC) 2006. *Federal plan for cyber security and information assurance research and development*. Arlington VA: NIST

Seger A 2005. A letter from the Council of Europe: cybercrime and organised crime. *Crime prevention and community safety* 7(4): 59–64