Cyber Security Incidents Outside Malaysia

Report No. 3 Feb 2007
NISER did not warrant the completeness or accuracy of the document and neither accepts any liability for losses howsoever incurred. The content on this site, including news, quotes, data and other information, is provided by third party content providers for your personal information only, and neither NISER nor its third party content providers shall be liable for any errors, inaccuracies or delays in content, or for any actions taken in reliance thereon.
DENIAL OF SERVICE

1. **Hackers slow Internet root servers with attack**

Online attackers have briefly disrupted service on at least two of the 13 "root" servers that are used to direct traffic on the Internet. The attack, which began Tuesday at about 5:30 a.m. Eastern time, was the most significant attack against the root servers since an October 2002 DDoS attack, said Ben Petro, senior vice president of services with Internet service provider Neustar. Root servers manage the Internet's DNS, used to translate Web addresses such as Amazon.com into the numerical IP addresses used by machines. The attack appeared to have been launched by a group of compromised PCs, called a botnet, Petro said. "Two of the root servers suffered badly, although they did not completely crash; some of the others also saw heavy traffic," said John Crain, chief technical officer with the Internet Corporation for Assigned Names and Numbers (ICANN). The two hardest-hit servers are maintained by the U.S. Department of Defense and ICANN, he added. The botnet briefly overwhelmed these servers with useless requests, causing them to occasionally hang, but did not disrupt Internet service, Petro said. By 10:30 a.m., Internet service providers were able to filter enough of the traffic from the botnet machines that traffic to and from the root servers was essentially back to normal. Compared to other DDoS attacks, this one did not have a lot of firepower. Petro said the bandwidth of the attack could be measured in megabytes, as opposed to the gigabyte-level attacks that are now frequently seen. "It was a small attack, but it was focused and targeted at the roots," he said.

Source: Infoworld, February 6, 2007
http://www.infoworld.com/article/07/02/06/HNrootserverattack_1.html

FRAUD

2. **Fraud vs id theft**

Fraud outstripped identity theft as the leading consumer complaint in Greater Cincinnati and Northern Kentucky for 2006, according to a new report by the Federal Trade Commission. Identity theft also was less common locally than nationally, the report showed. The FTC said in its annual report that identity theft accounted for 36 percent, or 246,035, of the national complaints. But locally, various forms of identity theft triggered 30 percent, or 1,205, of the complaints. ID theft complaints have leveled off after a steep increase earlier this decade. The number of ID theft complaints jumped from almost 162,000 in 2002 to a record 246,882 in 2004, slightly higher than last year's number, the agency said. Credit card fraud was the most common form of identity theft, the FTC said, making up 25 percent of the complaints, followed by phone or utilities fraud and bank fraud.

Source: Computer Crime Research Centre, Feb 11, 2007
3. **ISP head convicted in E-Rate fraud**

A U.S. federal jury convicted the former owner and president of ATE Tel Solutions Inc., a telecommunications and Internet service provider, on seven of nine counts of wire fraud in a scheme to defraud the E-Rate program, the U.S. Department of Justice said Friday. Rafael G. Adame was convicted of submitting fraudulent invoices for payment to the U.S. Federal Communications Commission's Universal Service Administrative Company. The E-Rate program provides subsidies to schools and libraries in poor, and often rural, areas of the U.S. so that they can afford Internet connectivity, computers and communications networks. Adame submitted the fraudulent invoices via wire communications when his company provided Internet services to schools in Texas. The federal jury that convicted him is in McAllen, Texas. He was found guilty of submitting fraudulent invoices via wire between December 2001 and May 2003, receiving US$106,514 in payments through the E-Rate program. Adame faces up to 20 years in prison for each count on which he was convicted and a $250,000 fine. He has not yet been sentenced.

Source: InfoWorld, February 12, 2007
http://www.infoworld.com/article/07/02/12/HNeratefraud_1.html

**HACK THREAT/INTRUSION**

4. **Vista hole opens door to 'shout hacking'**

The honeymoon ended early for Microsoft's Vista operating system, after word spread Wednesday about a flaw that could allow remote attackers to take advantage of the new operating system's speech recognition feature. Microsoft researchers are investigating the reports of a vulnerability that could allow an attacker to use the speech recognition feature to run malicious programs on Vista systems using prerecorded verbal commands, the company said in an e-mail statement. The potential security hole was discovered after an online discussion prompted blogger George Ou to try out a speech-based hack. Ou reported on ZD Net on Tuesday that he was able to access the Vista Start menu and, conceivably, run programs using voice commands played over the system's speakers. The speech recognition flaw is novel and notable for being the first publicized hole in the new operating system since the public launch of Vista on Tuesday. The impact of the flaw, however, is expected to be small. Vista users would need to have the speech recognition feature enabled and have a microphone and speakers connected to their system. Successful attackers would need to be physically present at the machine, or figure out a way to trick the computer's owner to download and play an audio recording of the malicious commands. Even then, the commands would somehow have to be issued without attracting the attention of the computer's owner. Finally, attackers' commands are limited to the access rights of the logged on user, which may prevent access to any administrative commands, Microsoft said in a statement.

Source: InfoWorld, February 1, 2007
http://www.infoworld.com/article/07/02/01/HNvistaspeechbug_1.html
5. **German police again the target of cybercrime**

Germany's Federal Criminal Police Office (BKA) is once again the target of criminal forces in the Internet. Spam e-mail allegedly sent by the police office is making the rounds in the German-speaking region of Europe. The e-mail contains an attachment with malware that has yet to be classified and is thus slipping by some antivirus programs, according to the BKA Web site. The subject line of the e-mail reads "Ermittlungsverfahren," or investigation. Recipients are informed that they face charges and should open the attached document, fill it out and return to the police office. Once opened, the malicious code affects some undisclosed functions of the user's PC and sends itself to the addresses listed in the user's address book. Telephone lines at the BKA were largely blocked Thursday as numerous recipients of the malicious spam called a telephone number listed in the e-mail that is the main number of the police's press office. In November, the BKA was the target of a similar malicious spam attack. This one involved an attachment with a worm also designed to automatically send itself to the addresses listed in the computer user's address book.

*Source: Infoworld, Feb 02, 2007*
http://www.infoworld.com/article/07/02/02/HNgermanpolicecybercrime_1.html

6. **Study: Weak passwords really do help hackers**

Left online for 24 days to see how hackers would attack them, four Linux computers with weak passwords were hit by some 270,000 intrusion attempts -- about one attempt every 39 seconds, according to a study conducted by a researcher at the University of Maryland. Among the key findings: Weak passwords really do make hackers' jobs much easier. The study also found that improved selection of usernames and associated passwords can make a big difference in whether attackers get into someone's computer. The study was led by Michel Cukier, an assistant professor of mechanical engineering and an affiliate of the university's Clark School Center for Risk and Reliability and Institute for Systems Research. His goal was to look at how hackers behave when they attack computer systems -- and what they do once they gain access. Using software tools that help hackers guess usernames and passwords, the study logged the most common words hackers tried to use to log into the systems. Cukier and two graduate students found that most attacks were conducted by hackers using dictionary scripts, which run through lists of common usernames and passwords in attempts to break into a computer. Some 825 of the attacks were ultimately successful and the hackers were able to log into the systems. The study was conducted between Nov. 14 and Dec. 8 at the school. Cukier was not surprised by what he found. "Root" was the top guess by dictionary scripts in about 12.34% of the attempts, while "admin" was tried 1.63% of the time. The word "test" was tried as a username 1.12% of the time, while "guest" was tried 0.84% of the time, according to the experiment's logs.

*Source: Computer World, February 6, 2007*
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9010540&intsrc=hm_list

7. **Hacker leaves explosions on nuclear website**

Red-faced officials at Canada's nuclear safety watchdog said they were probing how a hacker had managed to litter its official website with dozens of colour photographs
of a nuclear explosion. The Ottawa Citizen newspaper said every media release on the Canadian Nuclear Safety Commission’s website had been labelled as a security breach on Wednesday. When opened, each document had a headline reading ‘For immediate release’ and underneath was a large photo of an exploding atomic bomb. “We are in discussions with the (Internet service) provider. When we were informed the website had been tampered with, we immediately disabled the media module,” said commission spokesman Aurel Gervais, dismissing the suggestion that the hacker had been able to access secret information. The media site was working normally on Thursday. The Citizen — which published a colour photograph of one of the tampered pages — said the hacker had left a message saying ‘Please dont (sic) put me in jail ... oops, I divided by zero’. reuters

Source: Computer Crime Research Centre, February 12, 2007

8. **Attack by Korean hacker prompts Defense Department cyber debate**

Defense Department computer networks are probed and attacked hundreds of time each day. But a recent attack on the civilian Internet is causing DOD officials to re-examine whether the policies under which they fight cyber battles are tying their hands. “This is an area where technology has outstripped our ability to make policy,” said Air Force Gen. Ronald Keys, Commander of Air Combat Command. “We need to have a debate and figure out how to defend ourselves.” Unlike in the war on terror, DOD can’t go after cyber attackers who plan or discuss crimes until they act, Keys said. Web sites in other countries are beyond DOD’s reach, he added. “If they’re not in the United States, you can’t touch ‘em.” Keys said it would probably take a cyber version of the 9/11 attacks to make the U.S. realize that barriers to action in cyberspace should be re-evaluated. The danger is real, officials say. On Feb 5, an organized group of hackers perpetrated the most powerful set of attacks since 2002. The attacks targeted UltraDNS, the company that runs several servers that manage traffic for domains that end with .org and other extensions, according to several reports.

http://www.fcw.com/article97645-02-09-07-Web

9. **Cyber officials: Chinese hackers attack 'anything and everything'**

At the Naval Network Warfare Command here, U.S. cyber defenders track and investigate hundreds of suspicious events each day. But the predominant threat comes from Chinese hackers, who are constantly waging all-out warfare against Defense Department networks, Netwarcom officials said. Attacks coming from China, probably with government support, far outstrip other attackers in terms of volume, proficiency and sophistication, said a senior Netwarcom official, who spoke to reporters on background Feb 12. The conflict has reached the level of a campaign-style, force-on-force engagement, he said. “They will exploit anything and everything,” the senior official said, referring to the Chinese hackers’ strategy. And although it is impossible to confirm the involvement of China’s government, the attacks are so deliberate, “it’s hard to believe it’s not government-driven,” the official said. The motives of Chinese hackers run the gamut, including technology theft, intelligence gathering, exfiltration, research on DOD operations and the creation of dormant presences in DOD networks for future action, the official said. A recent
Chinese military white paper states that China plans to be able to win an “informationized war” by the middle of this century. Overall, China seeks a position of power to ensure its freedom of action in international affairs and the ability to influence the global economy, the senior official said.

Source: FCW.Com, February 13, 2007
http://www.fcw.com/article97658-02-13-07-Web

10. **Sandia backhacker wins $4.3 million judgment against Sandia Labs**

Shawn Carpenter, who was fired by Sandia National Laboratories in January 2005 for conducting backhacking operations against intruders he discovered on Sandia networks, won a $4.3 million wrongful discharge suit against the labs today. Backhacking occurs when networks are attacked and someone on the hacked network responds with a counterhack or attack. Carpenter, who worked in Sandia’s computer security operations organization, started detecting attacks against Sandia networks in 2002, according to court records in the 2nd District Court of New Mexico. Carpenter brought the attacks to the attention of Sandia and other government agencies, including the Army Research Laboratory and the FBI. Carpenter’s attorney, Thad Guyer, said testimony during the trial, which started Feb. 5, showed that Carpenter detected computer attacks from China, Brazil, Italy and Romania against Sandia systems. Guyer declined to say whether the attacks from China were state-sponsored, adding that he believed the attacks from the other countries were done in support of terrorist organizations. Despite Carpenter’s discovery of widespread hacking from abroad against Sandia networks, the lab decided to rein him in. This occurred, Carpenter alleged in the suit, despite the fact that he was cooperating with the FBI and the Army research lab in his backhacking investigation.

Source: FCW.Com, Feb 13, 2007
http://www.fcw.com/article97661-02-13-07-Web

WORM/VIRUS/TROJAN

11. **Super Bowl Site Hacked with Trojan, Keylogger**

Dolphin Stadium may be the site of this Sunday's Super Bowl XLI between the Bears and the Colts, but its Web site should be avoided like the plague. Bears, Colts and Super Bowl football fans everywhere beware. Users browsing the Internet, perhaps innocently looking up a seating chart at Dolphin Stadium in Miami, could be in a lot more trouble than they would have ever expected. Malicious code was discovered on the Web site for Dolphin Stadium, the location of this year’s Super Bowl, reports Websense. Websense Security Labs urged Web users to avoid that site completely until the site had been scrubbed cleaned of all destructive code. The code, hidden under the file name "w1c.exe," initiates both Trojan horse and keylogging capabilities, potentially allowing a hacker to track and record keyboard strokes in order to steal credit card, Social Security or other user information. The malicious JavaScript file was inserted into the header of the front page of the Dolphin Stadium site. Once visitors entered, it was designed to execute a script that attempts to exploit two known vulnerabilities: MS06-014 and MS07-004. Both of these exploits attempt to download and execute a malicious file. Given the popularity of the Super Bowl, the stadium site is linked from many official Super Bowl Web sites and related search
terms, which only intensified the Trojan horse's chances of affecting a large number of people. Websense notified the owners of the site.

Source: eWeek, February 2, 2007
http://www.eweek.com/article2/0,1895,2089951,00.asp

12. **CDC Web site attacked by virus**

Officials at the Centers for Disease Control and Prevention are concerned about a different kind of virus -- a computer one. Hackers broke into the C-D-C's Web site last week and planted a virus that could have infected visitors' computers. C-D-C officials said the hacking was concentrated to the agency's podcast site -- which has audio and video clips on a variety of public health topics -- and they do not think any sensitive information was compromised. The podcast site will be down for a few days. C-D-C officials encouraged visitors to the site to scan their computers for viruses. C-D-C spokesman Tom Skinner said the podcast site received several hundred visits in the few hours between when the virus entered the system on Thursday and when the site was deactivated. Skinner says the podcast site was launched in July and has received about 40,000 visits.

Source: Associated Press, February 5, 2007

13. **Botnet Stalkers Share Takedown Tactics at RSA**

A pair of security researchers speaking here at the ongoing RSA Conference Feb. 7 demonstrated their techniques for catching botnet operators who use secret legions of infected computers to distribute malware programs and violent political propaganda. The botnet experts, both of whom are employed by anti-malware software maker FaceTime Communications, based in Foster City, Calif., detailed how they identified and pursued individuals believed to be responsible for running a pair of sophisticated botnet schemes, which have been subsequently shut down or significantly scaled back. Addressing a packed room of conference attendees, Chris Boyd, director of malware research at FaceTime Security Labs, and Wayne Porter, director of special research for the company, detailed their efforts to infiltrate the botnet community and find the people responsible for running underground networks believed to have harbored as many as 150,000 compromised computers. One of the botnets uncovered by the researchers was based in the United States and was used to deliver malware code including spyware that stole credit card data from e-commerce systems for the purpose of committing fraud. The other crimeware distribution campaign appears to have been used by radical Middle Eastern ideologists to espouse violent messages of world domination and steal money to buy satellites, radios and computer equipment.

Source: eWeek, February 8, 2007
http://www.eweek.com/article2/0,1895,2092435,00.asp

14. **Spyware, data privacy bills reappear in House**

In October 2004, all but one member of the U.S. House of Representatives voted for a bill that was supposed to curtail the threat of malicious PC-disrupting spyware. But the Senate ignored it. So the House once again approved spyware regulations in
May 2005, which yielded precisely the same lack of a result. Hoping that the third time proves the charm, House leaders on Thursday introduced a bill that would once again try to impose 31 pages of regulations on the software industry in an effort to define what types of activities are permissible and which ones aren't. Rep. John Dingell, a Michigan Democrat and the chairman of the House Energy and Commerce Committee, called the announcement "a serious down payment on resolving the scourge of identity theft and related abuse." He promised that legislation would be sent to the House floor "expeditiously." Dingell was referring not only to the spyware measure but also to three other proposals announced at the same time: a bill to regulate telephone pretexting, one to curb the sale of Social Security numbers, and one to impose many additional security requirements including data breach notifications on private companies (though not federal agencies). Taken together, the measures represent a broad and surprisingly bipartisan attempt by House leaders to rewrite many electronic privacy laws.

Source: CNet News, February 8, 2007

15. Anatomy sheds new light on Storm Worm

A deluge of Trojan-laced spam that slyly tricked recipients by promising information about winter storms ravaging Northern Europe last month was even more crafty than we thought. Among the new revelations: The Storm Worm malware launched DDoS attacks on a host of websites related to spam, antispam and just about anything else that may have piqued the perpetrators' ire, according to Joe Stewart, senior security researcher for SecureWorks. It also appears to be a close descendant of worms that spread in November and December, a connection that few if any have made until now. Storm Worm captured the grudging admiration of those in the security industry for its uncanny ability to marry technical prowess with social networking. Within days of brutal storms sacking Europe, the email assault began bearing subject lines such as "230 dead as storm batters Europe." Sadly, plenty of recipients fell for the topical come-on. Over the next week, the worm played at least a half dozen variations on a theme, using subjects such as one claiming US Secretary of State Condoleezza Rice kicked German Chancellor Angela Merkel. It was known to install a root kit that made victims part of a botnet. Stewart says Storm Worm is a variant of the Win32/Nuwar worm that spread as early as November. Unbeknown to most at the time, Storm Worm also also installed a DDoS attack tool that wreaked havoc on various websites. Among them was spammation.info, which is dedicated to countering the menace of spam. According to a February 3 posting, the site was shut down for eight days by a DDoS attack suspected to have been carried out by "spammers who were unhappy about the fact that the site publishes information about stock spam". Other sites that were also targeted by Storm Worm included stockpatrol.com and several sites Stewart guesses were run by rival spammer gangs.

Source: The Register, February 9, 2007
http://www.theregister.co.uk/2007/02/09/storm_worm_anatomy/

16. Penn State Researchers Develop New Worm-Stopping Technology

Researchers at Penn State University say they have developed anti-malware technology that can identify and contain worms in milliseconds rather than minutes -- greatly limiting how far they spread and how much damage they cause. The new
technology, Proactive Worm Containment, focuses on analyzing packet rate and frequency of connections, rather than signature or pattern identification, according to a release from Penn State. "A lot of worms need to spread quickly in order to do the most damage, so our software looks for anomalies in the rate and diversity of connection requests going out of hosts," says Peng Liu, associate professor of information sciences and technology at Penn State and lead researcher on the Proactive Worm Containment system. Penn State researchers assert that because many security technologies focus on signature or pattern identification for blocking worms, they cannot respond to new attacks fast enough, allowing worms to exploit network vulnerabilities. Several minutes can elapse between when a signature-based system first recognizes a new worm and when it creates a new signature to block it from spreading any more.

Source: Information Week, Feb 12, 2007
http://www.informationweek.com/showArticle.jhtml;jsessionid=MIRYBBI1UOICGQSNDLRCKH0CJUNN2JVN?articleID=197005266

17. 'Storm Trojan' ignites worm war

The Trojan horse that pumped up spam volumes in January is at it again, researchers said today, and is now spreading over instant messaging and engaging in attacks on rival malware. Symantec Corp. researchers said that the "Storm Trojan," a.k.a. "Peacomm," is now spreading via AOL Instant Messenger (AIM), Google Talk and Yahoo Messenger. An alert to some Symantec customers pegged the new infection vector as "insidious" because the message -- such as the cryptic "LOL ;)") -- and the included URL can be dynamically updated by the attacker. Even worse, according to Alfred Huger, senior director of Symantec's security response team, "it injects a message and URL only into already open windows. It's not just some random message that pops up, but it appears only to people [you are] already talking to. That makes the approach very effective." Moreover, the server from which the malware is downloaded to the victim's PC can be quickly changed by the attacker using the Trojan's peer-to-peer (P2P) control channel. "Everything can constantly change," said Huger. The newest attack by Peacomm follows an earlier campaign in January, when the Trojan got its nickname from e-mail subject headings that touted news of massive storms throughout Europe. But one researcher traced the Trojan further back than that. According to an analysis by Joe Stewart, a SecureWorks senior security researcher, Peacomm is actually a spinoff of last year's "Nuwar" worm. "It's pretty much the same code," said Stewart. Both Stewart and Huger also noted that the Trojan has been behind several recent distributed denial-of-service (DDoS) attacks against antispam Web sites, as well as servers supporting rival malware.

Source : Computer World, February 12, 2007
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011146&intsrc=hm_list

18. China Detains Six over 'Panda' Computer Virus

China has detained six men in their 20s for writing or profiting from a computer virus dubbed the "joss-stick burning panda" which has infected over a million PCs in the country, local media said on Wednesday. The worm wreaked havoc among individual and corporate users in China in a late 2006 outbreak, deleting files, damaging programs and attacking web portals. It got its name from changing icons
on desktops into cute cartoon pandas, the most famous of which holds three burning joss-sticks in his paws. Chinese media have said that the worm was able to steal account names of online gamers and instant messengers, which are hotly traded with real money in China's cyberspace. Police held Li Jun, 25 a native of Wuhan city in central China, who wrote the virus in October and had earned more than 100,000 yuan ($12,890) by selling it to about 120 people, the Beijing News said. The other five, from three different provinces, were detained for updating and spreading the virus or for profiting from the stolen account names, the Beijing News said. "It is the first time our country has cracked a major computer virus case," it added.

Source : eWeek, February 13, 2007
http://www.eweek.com/article2/0,1895,2094418,00.asp

19. Valentine worm 'spreading fast'

Security experts today warned that a "widespread worm" posing as a Valentine's greeting is spreading fast across the internet. Dref-AB has been deliberately spread so that office workers and home computer users find the malicious email in their inbox first thing this morning. Since midnight GMT Dref-AB has accounted for 76.4 per cent of all malware sighted at Sophos' global network of virus monitoring stations. Subject lines used in the attack are many and varied, but all pose as a romantic message. Some of them include: 'A Valentine Love Song', 'Be My Valentine', 'Fly Away Valentine', 'For My Valentine' and 'Happy Valentine's Day'. The worm is attached to the emails in files called 'flash postcard.exe', 'greeting postcard.exe', 'greeting card.exe', or 'postcard.exe'. "This new Valentine attack is spreading fast across the net, accounting for over three quarters of all the malware we've seen at email gateways around the globe since 14 February began," said Graham Cluley, senior technology consultant at Sophos.

Source: VNuNet, Feb 14, 2007

SPAM

20. Valentine's spams a-plenty, but this year spammers face a harder sell 5% of computer users admit to purchasing goods sold via spam

In the run-up to Valentine's Day, Sophos has reported seeing a rise in the number of spam campaigns selling romantic gifts such as jewelry, chocolate and lingerie. However, a new Sophos poll reveals that just five percent of computer users now admit to purchasing goods sold via spam*, compared to nine percent this time last year. "The results are in - spammers are no longer facing such an easy ride when it comes to flogging goods, whether they're personalized Valentine's Day gifts or the latest and greatest in ten-day weight-loss medication," said Graham Cluley, senior technology consultant at Sophos. "The simple fact is that if no-one bought goods sold via junk email the spammers would stop. It's encouraging to see a drop in the number of people who own up to making purchases, but with the number of email users worldwide, five percent is still more than enough to keep the spammers in business."

Source : Sophos, Feb 12, 2007
Advances in IT over the decades have come mostly in small increments — Release 2.3 yields to 2.4, transistors shrink a few more nanometers, Ethernet gets another speed boost, bugs are fixed, and algorithms get tweaked. That kind of evolutionary approach has served users well, boosting speeds, capacities and application capabilities by many orders of magnitude. But such incremental improvements are no longer sufficient to keep the Internet viable, according to a growing number of researchers. In fact, they say, the Internet is at the tipping point of overwhelming abuse and complexity. The most sanguine of observers say that even if the Internet is able to avoid some kind of digital Armageddon brought on by spammers, hackers, phishers and cyberterrorists, it nevertheless will drown in a flood of mobile gadgets, interactive multimedia applications and Internet-enabled devices, including phones, cars, home appliances and radio frequency identification tags. Indeed, researchers say, it is time to rethink all the old notions from the late 1960s and 1970s when the Internet was in its infancy. While few think it is possible to literally start over, there are a number of so-called clean-slate research programs that start with the premise that anything is possible and no option is too far out to consider. Nick McKeown, a computer scientist at Stanford University, heads up one such program. He says the Internet is “broken” in at least two places — security and mobility.

Source: Computer World, February 12, 2007
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=279934&intsrc=hm_ts_head

OTHERS

22. German court bans police from spying on PCs

Germany's High Court has handed down a landmark decision banning police from installing spyware on computers of suspected criminals without their knowledge. The decision, announced Monday, is a blow to the plans of the German Interior Minister Wolfgang Schäuble to give the Federal Criminal Police Office (BKA) greater power to monitor terrorists and other criminals online, and peek inside their computers. Two other federal judges had differed over whether police should be able to hack into the computers of suspected criminals and install spyware. In February, one judge approved police hacking. But another barred the practice in November, resulting in an appeal by federal prosecutors. The High Court in Karlsruhe argued that searching computers is similar to searching homes, a practice in Germany that requires police to follow certain procedures, such as obtaining a search warrant and informing suspected offenders of a search. The judges also argued that hacking computers by the police is not permitted under Germany's strict phone-tapping laws and that legislation would be needed to enable covert surveillance.

Source: Infoworld, February 5, 2007
http://www.infoworld.com/article/07/02/05/HNbanpolicefromspying_1.html
23. **Price of cybercrime tools shrinks**

It's becoming cheaper and easier to get hold of the tools needed to launch a cybercrime attack, according to security company RSA. Jens Hinrichsen, the company's product marketing manager for fraud auction, said Thursday that RSA has been monitoring the Web sites and ICQ channels where malicious hackers and cybercriminals interact. These sites allow participants to share feedback and even review one another's products. Addressing an audience at the RSA Conference 2007 here, Hinrichsen showed several screen grabs to illustrate that the prices being asked for hacking tools have been dropping, with many participants embracing volume discounts and other incentives. One example was a post offering a "Super Trojan," which could be used to install malicious code on a victim's PC, for $600. "What's interesting is that this is actually a reviewed vendor, who actually had a lot of good transactions. He's offering this custom piece of crimeware for only $600," said Hinrichsen, who added that he "loved the term 'Super Trojan.'" "So, when we talk about the ever-increasing ramp-up of more sophisticated tools," he said, "the prices are coming down."


24. **Safety of online banking**

An initiative by Standard Bank to tighten the safety of online banking has failed, with fewer than one in seven customers bothering to use the security software. The bank launched its security pin pad feature after money was filtered out of accounts by using keystroke logging software, which records the personal identity number (PIN) typed in by customers. The bank's solution in 2003 was to display a small picture of a keyboard on the log-in screen, so users could click on the relevant numbers to enter their PIN instead of typing it. But the feature has been removed because of apathy by the clients it aimed to protect. The apathy shows that while users expect online activities to be secure, they oppose any inconvenience or changes to their own habits. The bank says its transactions are still secure as it has now made it compulsory to use a one-time password, where a unique code is delivered by SMS when a user initiates a banking session.


25. **US government readying massive cybersecurity test**

The U.S. Department of Homeland Security (DHS) is planning a large-scale test of the nation's response to a cyberattack to be held in early 2008. The test will be a follow-up to the February 2006 Cyber Storm test, which was billed as the largest-ever U.S. government online attack simulation. Cyber Storm 2 will be conducted in March 2008, said Gregory Garcia, assistant secretary for cyber security and telecommunications with DHS, speaking at the RSA Conference in San Francisco last week. Like the first Cyber Storm, this exercise will evaluate the ability of the public and private sector to provide a coordinated response to a large-scale cyber event, he said. The second Cyber Storm test, which is in the planning stages right now, will include a greater number of participants than its predecessor, said Tiffany Jones, senior regional manager for government relations with Symantec. In
particular, the number of international participants will be increased, she said. Symantec was one of about 30 corporations that participated in the first exercise and will again be involved in Cyber Storm 2, she said. The first Cyber Storm drew 115 organizations from the U.S., Canada, the U.K., Australia, and New Zealand. Participants included Microsoft, Verisign, the U.S. Department of Defense, the U.S. Department of Justice, the U.S. State Department, and the U.S. National Security Agency. Next year's test is expected to bring in corporate players from outside of the IT industry that were not involved in the first exercise -- transportation and chemical companies for example, Jones said. She said that the DHS plans to host further Cyber Storm events beyond 2008 on a biannual basis.

Source: InfoWorld, February 12, 2007
http://www.infoworld.com/article/07/02/12/HNcyberstorm2_1.html