CYBER SECURITY INCIDENT
OUTSIDE MALAYSIA

Report No. 11 – June 2007

30 June 2007

CyberSecurity Malaysia
(formerly known as NISER)
Level 7, SAPURA@MINES
No 7, Jalan Tasik
Mines Resort City
43300 Seri Kembangan
Selangor

Tel +60 3 8992 6888
Fax +60 3 8945 3205

http://www.cybersecurity.org.my

Securing Our Cyberspace

An agency under

Ministry of Science, Technology & Innovation
TABLE OF CONTENT

FRAUD
1. Dutch police arrest 111 West Africans in 419 clampdown ............................................. 1
2. Internet fraud victims ............................................................................................................. 1
3. eBay targets Romanian fraudsters ....................................................................................... 1

HACK THREAT/INTRUSION
4. Humans, not tech, are the greatest security risk ............................................................... 2
5. A million zombies threaten US national security .............................................................. 2
6. Cyber crooks hijack 10,000 websites .................................................................................... 3
7. Hacker successfully attacks 10000 websites ..................................................................... 3
8. Hackers use 'construction kit' to unleash Trojan variants .................................................. 3
9. Hackers Take Over MySpace Pages To Build Bots ............................................................ 4

WORM/VIRUS/TROJAN
10. Botnet Battle a 'Game of Whack-a-Mole' ................................................................. 4
11. Global co-op feeds FBI's botnet fight .................................................................................. 5
12. Crippling malware attack strikes in Italy .......................................................................... 5
13. Business of computer viruses ............................................................................................ 5
14. Shockwave as Trojan horse uses animated disguise Windows users risk being duped by animation smokescreen ................................................................. 6
15. Don't download Microsoft Security Bulletin MS07-0065! Malicious spam posing as fake vulnerability patch leads to Trojan horse infection .............................................. 6
16. Harry Potter worm claims teenage wizard is dead ............................................................ 6

SPAM
17. Spam costs $2.5 million in damages .................................................................................. 7
18. “Dirty Duo” found guilty of operating sexually explicit spam business Jury convicts two men on charges including conspiracy, money laundering, fraud and transportation of obscene materials .......................................................................................... 7

OTHERS
19. German Flickr censorship causes web outcry ............................................................. 8
20. George W. Bush vs cybercrime .......................................................................................... 8
21. Increase in cyberthreats spurs feds, industry ................................................................. 8
22. Cyber-baddies doing our heads in .................................................................................... 9
23. Border agencies prep for multi-modal biometrics ............................................................ 9
DISCLAIMER

This document is a non-commercial publication intended to educate and disseminate information about security incidents reported outside Malaysia. Further reproduction or redistribution is subject to original copyright restrictions. CyberSecurity Malaysia provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

CyberSecurity Malaysia 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 CyberSecurity Malaysia 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.
FRAUD

1. **Dutch police arrest 111 West Africans in 419 clampdown**

Dutch police have arrested 111 suspected 419 scammers. The arrests on Saturday follow the end of a seven-month investigation - dubbed Operation Apollo, AFP reports. Eight of those detained were carrying false papers. Many others among the group of West African (mainly Nigerian) suspects are reckoned to have entered the Netherlands illegally or to have overstayed their permitted stay. The alleged scammers are suspected of running a series of lottery-based (AKA 419-lite) scams. Prospective victims of these frauds are first informed by email that they have won fictitious lottery prizes. Victims are then tricked into handing over money-up front to cover processing fees or other fictitious expenses. The promised windfalls never materialise and dupes are left nursing their losses. Investigators in the Netherlands estimate that 2,000 internet con-men are active in the country.

**Source:** The Register, June 19, 2007
http://www.theregister.co.uk/2007/06/18/dutch_arrest_419_suspects/

2. **Internet fraud victims**

Otherwise smart people are still being duped into spending big money to collect imaginary lottery winnings in Internet scams. Since the Trinidad Express reported last Christmas on a money scam originating in Australia and conning dozens of locals, three more embarrassed people have come forward to report being robbed. The victims were using the Internet when they received pop-up advertisements inviting them to play lottery. The victims said they played and days later received an e-mail informing them they had won. The money, they were told, would be delivered after they paid lottery taxes and legal fees. The three spent more than 4,000 pounds sterling and never received a dollar of their “winnings”. Most people ignore the spam e-mails, which often originate in Nigeria, Holland, and recently Russia and Italy. The sender tells a version of an old con-a dead millionaire leaving behind an unclaimed fortune in a bank with no heirs, and your help being needed to claim it, or to transfer the funds.

**Source:** Computer Crime Research Centre, June 25, 2007

3. **eBay targets Romanian fraudsters**

Online auction site eBay has made public the details of a three-year long campaign to curb online fraud being perpetrated by criminals in Romania—an effort that has resulted in several hundred arrests. Matt Henley, a member of eBay's US-based Fraud Investigations Team, spoke about the campaign while taking part in a two-day workshop in Sydney with representatives of local law enforcement agencies. Henley is currently in town to discuss the latest online fraud techniques with representatives from the Australian Federal Police, the High-Tech Crime Centre, the Australian Crime Commission, ACMA and all the State and Territory Police forces. The e-
commerce site’s internal fraud team first took note of a higher than usual amount of fraudulent activity from Eastern Europe in 2005.

Source: ZDNet Australia, June 27, 2007

**HACK THREAT/INTRUSION**

4. **Humans, not tech, are the greatest security risk**

The Department of Trade and Industry has made £4million (RM27.2 million) available for four research projects aimed at reducing the IT risk created by human error. The programme, which is part of its Network Security Innovation Platform, reflects the fact that human error is by far the biggest risk to network security, the DTI said. It cited the results of a survey it conducted, involving over 1,800 people, on the use of passwords. It found that:

- Just over one third recorded their password or security information by either writing it down or storing it somewhere on their computer
- Nearly two thirds never changed their password
- One in five people used the same password for non-banking websites as well as their online bank

The projects will use behavioural science in a bid to tackle the human risk element in network security. Four projects will receive funding under the programme. The first, to be carried out by BAE Systems and Loughborough University, involves developing a risk assessment package focused on organisational and human factors.

Source: The Register, June 18, 2007
http://www.theregister.co.uk/2007/06/18/dti_it_security_research/

5. **A million zombies threaten US national security**

More than a million PCs under the control of spammers are threatening the US national security, its economy and its information infrastructure, according to the FBI. The discovery was made by Operation Bot Roast, which is an initiative aimed at revealing the scale of the botnet problem and prosecuting those responsible. It is being carried out in conjunction with Carnegie Mellon University, Microsoft and the International Botnet Task Force. Botnets are collections of computers—known as bots or zombies—whose respective owners have no idea their PCs have been hijacked and are being used for identity theft, denial-of-service attacks and the transmission of malware and spam. The FBI claims that botnets are a “growing threat to national security, the national information infrastructure, and the economy” in the US. The assistant director for the FBI’s Cyber Division, James Finch, urged computer users last week to “protect themselves from botnets and the associated schemes by practising strong computer security habits”.

Source: ZDNet Australia, June 18, 2007
6. **Cyber crooks hijack 10,000 websites**

More than 10,000 websites have been infected by a sophisticated and fast-acting Trojan downloader that attempts to install malware on visiting PCs. At least one security firm, Trend Micro, is working with the FBI to contain the damage and track down the perpetrators. The attack is noteworthy for the number of sites it has managed to infect in a relatively short period of time. Between Friday and Sunday night, the number jumped from 1,100 to about 2,500. By Monday afternoon, California time, there were more than 10,000 infected sites, according to Paul Ferguson, a network architect for Trend Micro. Once a server is infected, attackers embed an invisible iframe into the web page that silently redirects visitors to a pair of other sites that attempt to use previously patched Windows vulnerabilities to install malicious keylogging software. The redirected sites use an attack kit known as MPack, which according to this writeup from Symantec is “a professionally written collection of PHP software components designed to be hosted and run from a PHP server with a database backend.” Researchers are still trying to figure out how the attackers have managed to infect the servers. “It’s all over the map,” Ferguson says. “The sheer numbers right now are keeping us pretty busy.”

**Source:** The Register, June 19, 2007  
http://www.theregister.co.uk/2007/06/18/hijacked_sites_install_malware/

7. **Hacker successfully attacks 10000 websites**

Attackers armed with an exploit tool kit have launched massive attacks in Europe from a network of at least 10,000 hacked Web sites, with infections spreading worldwide, several security companies warned today. As early as last Friday, analysts reported the opening salvos of a large-scale attack based on the multiexploit hacker kit dubbed “Mpack.” The mechanics of the attacks are complex, but essentially attackers taint each compromised site with code that then redirects visitors to a server hosting the Mpack kit—a professional, Russian-made collection of exploits that comes complete with a management console to detail which exploits are working and against what countries’ domains. Infected computers are fed a diet of malicious code, largely keyloggers that spy out usernames and passwords for valuable accounts such as online banking sites.

**Source:** Computer Crime Research Centre, June 24, 2007  

8. **Hackers use ‘construction kit’ to unleash Trojan variants**

Multiple hacker groups are using a “construction kit” supplied by the author of a Trojan horse program discovered last October to develop and unleash more dangerous variants of the original malware. Already such variants have stolen sensitive information belonging to at least 10,000 individuals and sent the data to rogue servers in China, Russia and the U.S., according to Don Jackson, a security researcher at SecureWorks Inc. in Atlanta. The stolen data includes Social Security numbers, online account information, bank account
and credit card numbers, usernames and passwords, and other data that users would usually input during an SSL session. The Prg Trojan, as it has been dubbed by SecureWorks, is a variant of another Trojan called wnspoem that was unearthed in October. Similar to wnspoem, the Prg Trojan and its variants are designed to sniff sensitive data from Windows internal memory buffers before the data is encrypted and sent to SSL-protected Web sites. The Trojans are programmed to send the stolen data to multiple servers around the world where it is stored in encrypted fashion and sold to others looking for such information. An analysis of log files on the servers storing the stolen data shows that a lot of the information is coming from corporate PCs, Jackson said.

http://www.computerworld.com/action/article.do?command=viewArticleBasic &articleId=9025735&intsrc=hm_list

9. Hackers Take Over MySpace Pages To Build Bots

Internet Storm Center researchers are warning users that drive-by exploits have been embedded in a few dozen legitimate MySpace pages. Johannes Ullrich, chief technology officer with the Internet Storm Center, told InformationWeek that the malicious code that’s embedded in the Web pages installs the FluxBot, a dangerous new bot. Since the bot doesn’t have a central command and instead relies on a complex set of ever-changing networks of proxy servers, Ullrich said it’s extremely difficult to shut it down or cleanse it off an infected system. “It appears that these are compromised accounts,” said Ullrich. “Hackers overtook maybe a few dozen pages. MySpace is fixing the issue. ... They reacted very quickly in this case.”

http://www.informationweek.com/security/showArticle.jhtml;jsessionid=B50 NC0JHNDDKAQSNDLRSKHSCJUNN2JVN?articleID=200001122

WORM/VIRUS/TROJAN

10. Botnet Battle a 'Game of Whack-a-Mole

No one ever said policing the Internet was easy. Bot herders control networks of compromised computers sometimes numbering into the thousands. Already, an FBI-led initiative dubbed “Operation Bot Roast” has identified 1 million compromised computers. On Wednesday, FBI officials laid out charges against three men—Robert Alan Soloway of Seattle, James C. Brewer of Arlington, Texas, and Jason Michael Downey of Covington, Ky.—as part of Operation Bot Roast. But security professionals say bot herders are growing increasingly sophisticated as they search for ways to thwart their opponents. Officials at Sunnyvale, Calif.-based Mi5 Networks reported seeing bots that connect to multiple command and control servers as well as bots that scan internal networks for different vulnerabilities and then only deliver the exploit payload for which the specific machine is vulnerable. Battling botnets, said Mi5 CEO Doug Camplejohn, has officially turned into a “game of Whack-a-mole.”
11. **Global co-op feeds FBI's botnet fight**

Officials with the FBI claim that global law enforcement partnerships are playing a significant role in its ongoing efforts to stomp out botnets and other computer-borne crimes. Security researchers have long maintained that one of the most significant obstacles to shutting down botnets is the distributed global nature of the individuals responsible for operating the networks of zombie PCs. Botnets are banks of computers infected by virus programs that allow them to be secretly used to carry out many forms of electronic attacks. The conventional wisdom has been that U.S. law enforcement officials have struggled to find the budget and manpower necessary to track down cyber-criminals operating on their own turf, let alone find a way to identify and arrest people distributing malware code or operating botnets who are based in foreign nations. However, hot on the heels of its announcement of a round of arrests of U.S.-based botnet herders and the identification of over one million machines infected by the programs, FBI officials said that international cooperation is playing an increasingly important role in helping it stomp out cyber-crime.

Source: Department of Homeland Security, June 18, 2007  
http://www.eweek.com/article2/0,1895,2146554,00.asp

12. **Crippling malware attack strikes in Italy**

Italy is suffering from a barrage of remote attacks launched from hundreds of compromised websites, security experts have warned. Researchers at Symantec reported that attackers have injected 'iframe' tags within the HTML files on compromised sites. The tags redirect users to a site that runs MPack, a utility that attempts multiple exploits and malware installations. More than 65,000 users had been redirected to the malicious page since Friday afternoon, and more than 7,000 successful exploits had been carried out. Symantec researcher Elia Florio warned in a company blog that users should update antivirus software and all system and third-party software that can be vulnerable to attacks.


13. **Business of computer viruses**

A new computer virus was identified last week that spreads via USB flash drives and other removable media on Windows PCs. This method of propagation is about as old as computers themselves. So what’s the big deal? It’s the content of the program that makes this particular virus so special. The worm doesn’t infect a computer with maladjusted software or erase important system files. Instead, it spreads educational information about
HIV/AIDS. Security experts have been quick to point out that the worm, called “liarVB-a,” does no explicit harm to the user’s computer, but it’s still a potential security threat.

Source: Computer Crime Research Centre, June 23, 2007

14. **Shockwave as Trojan horse uses animated disguise** Windows users risk being duped by animation smokescreen

The Trojan horse plays a Shockwave animation by Italian cartoonist Bruno Bozzetto. Experts at Sophos, a world leader in IT security and control, have discovered a Trojan horse that disguises its malicious intent by playing a humorous animation. The Troj/Agent-FWO Trojan horse plays the popular “Yes & No” Shockwave video created by the Italian animator Bruno Bozzetto, but only after embedding itself on users’ computers and downloading further malicious code from the internet. “Yes & No”, which was published on the internet by Bozzetto in 2001, is a humorous video about how obeying the rules of the road does not always make sense. Hundreds of thousands of people are believed to have watched the online animation. According to Sophos experts, the Trojan horse is playing the animation as a smokescreen as it silently infects Windows computers.


15. **Don’t download Microsoft Security Bulletin MS07-0065! Malicious spam posing as fake vulnerability patch leads to Trojan horse infection**

Experts at Sophos, a world leader in IT security and control, have warned of a widespread attempt to infect email users by sending them a warning about a bogus Microsoft security patch. The emails, which have the subject line “Microsoft Security Bulletin MS07-0065” pretend to come from Microsoft, and claim that a zero-day vulnerability has been discovered in the Microsoft Outlook email program. They go on to warn recipients that “more than 100,000 machines” have been exploited via the vulnerability in order to promote medications such as Viagra and Cialis. Users are encouraged by the email to download a patch which, it is claimed, will fix the problem and prevent them from becoming attacked by hackers. However, clicking on the link contained inside the email does not take computer users to Microsoft’s website but one of many compromised websites hosting a Trojan horse. Sophos proactively detects the Trojan, without requiring an update, using Behavioral Genotype® Protection as Mal/Behav-112.


16. **Harry Potter worm claims teenage wizard is dead**

With just weeks remaining until the release of the last ever Harry Potter novel, and the imminent premiere of the fifth movie in the franchise, Sophos has warned of a new computer worm exploiting Potter-mania around the world. The W32/Hairy-A worm can automatically infect a PC when users
plug-in USB drives, which carry a file posing as a copy of the eagerly anticipated novel, “Harry Potter and the Deathly Hallows”. If the users have allowed USB drives to ‘auto-run’ they will see a file called: HarryPotter-TheDeathlyHallows.doc. Inside this Word document file is the simple phrase “Harry Potter is dead.” The worm then looks for other removable drives to infect.


SPAM

17. **Spam costs $2.5 million in damages**

In a case of justice gone horribly wrong, WebGuy.net’s Mark W. Mumma, ISP, spam victim and anti-spam activist, has been dealt the ultimate “low blow” by a Federal Court. The small, Oklahoma City based ISP has been ordered by a U.S. Federal Jury to pay $2.5 Million in damages to the very company that admitted sending him unsolicited e-mail in the first place. Oklahoma City, OK (PRWEB) June 27, 2007 -- In a mind numbing decision two months ago today in case no. 05-CV-122 in the U.S. District Court’s Eastern District of Virginia, Judge Leonie M. Brinkema ruled that Mark W. Mumma’s statement that Plaintiffs, Cruise.com, Omega World Travel and Gloria Bohan “are spammers” is “untrue” in spite of the fact that Cruise.com witnesses confirmed, under oath, that they never ask a recipient’s permission prior to sending them e-mail offers. The reason given by Cruise.com CEO Anthony Hamawy regarding why they don’t verify an e-mail recipient’s desire to receive their offers was, ‘No, we have not, primarily because our competitors don’t.’

Source: Computer Crime Research Centre, June 27, 2007
http://www.crime-research.org/news/27.06.2007/2750/

18. **“Dirty Duo” found guilty of operating sexually explicit spam business** Jury convicts two men on charges including conspiracy, money laundering, fraud and transportation of obscene materials

James Schaffer and Jeffrey Kilbride ran an international pornographic spam business. Experts at IT security and control firm Sophos have welcomed news that two men have been found guilty for their part in an international spam gang which bombarded innocent internet users with graphic pornographic images. A federal jury has convicted James R. Schaffer, of Paradise Valley, Arizona, and Jeffrey A. Kilbride, of Venice, California, on charges including conspiracy, money laundering, fraud and transportation of obscene materials. Spam sent by Schaffer and Kilbride is said to have resulted in America Online receiving more than 600,000 complaints from users between 30 January and 9 June 2004. The spam messages were sent out to promote hardcore pornographic websites, and according to Assistant Attorney General Alice Fisher grossed the two men, both 41 years old, more than $2 million.


OTHERS

19. **German Flickr censorship causes web outcry**

Flickr’s introduction of content filters in Germany last week has provoked protests in blogs and web forums globally. While in most countries the photo sharing site’s “SafeSearch” function can be turned off by users interested in seeing all the photos available on Flickr, that option has been axed in Germany due to “stricter legislation and penalties in that country”, parent company Yahoo! said in a statement. Yahoo! says it isn’t about censorship and that it is trying to improve the use of filters while still complying with German law. The limitations were introduced because German law requires websites to verify that visitors are old enough to see potentially sensitive content, such as erotic photos. Users are now calling for boycotts. One group, Against Censorship at the Flick, even created a pool of images that German users are not allowed to see. The reactions have surprised both Flickr and Yahoo!. “We apologise that this happened in the first place, and we’d like to have more to say: there’s almost nothing in the world that I’d enjoy doing less than deciding what grown-up Germans are or are not allowed to look at,” one Flickr staff member said. Flickr encountered similar criticism when some of its photos were blocked in the United Arab Emirates and China.

Source: The Register, June 19, 2007
http://www.theregister.co.uk/2007/06/18/outcry_against_flickr_censorship/

20. **George W. Bush vs cybercrime**

President George W. Bush on Monday highlighted the growing danger of cyberattacks, in a meeting with his Estonian counterpart Toomas Ilves, whose country recently was hit hard by the crimes. “We also talked about an interesting subject, and one that I can learn a lot about, and that is the cyberattack that makes us all vulnerable,” Bush said, adding “this President (Ilves), one, understands the issue well; two, has got some ideas, including a NATO center of excellence in Estonia to deal with this issue.” Estonia recently say cyberattacks deal setbacks to many of the country’s computer networks. It has accused Russian neighbors of using the weapon just as bilateral ties are severely strained.

Source: Computer Crime Research Centre, June 26, 2007

21. **Increase in cyberthreats spurs feds, industry**

A reinforced cadre of federal cybercrime prosecutors and technicians at the third annual GFirst conference marshaled new deterrents and defenses against the rising level of cyberattacks, as industry executives forecast increases in the market for security products. More than 550 people from
about 70 organizations attended the conference, including dozens from the Justice Department’s Computer Hacking and Intellectual Property Coordinators’ Conference. The CHIPS attendees convened several closed meetings to discuss investigative and legal strategies against cybercrime. CHIPS has grown from five prosecutors in 1991 to more than 240 DOJ attorneys, including two prosecutors in each regional office and a headquarters team in Washington, officials said. CHIPS members provide technical and legal support to other prosecutors and Justice officials. Greg Garcia, the Homeland Security Department’s assistant secretary for cybersecurity and communications, said his organization had received more than 21,000 reports of cyber incidents through May during this fiscal year, in contrast to about 24,000 during all of 2006.


22. **Cyber-baddies doing our heads in**

A study finds cybercriminals using mind games to get our info and cash. Security software company McAfee has announced findings from new research revealing how organised crime is employing psychological mind games to trick PC users into handing over personal information and money. The investigation into cybercrime trends suggests Internet fraudsters are exploiting our deepest psychological vulnerabilities in the latest email scams. such as assuming trustworthy identities, engaging in friendly banter and targeting human emotions such as fear, insecurity and greed. Stupidity also seems to be an ally of the cyber rotters; When an online ad promised to infect the computers of all those that clicked with a virus, 400 people still did exactly that.

Source: Computer Crime Research Centre, June 28, 2007

23. **Border agencies prep for multi-modal biometrics**

The UK, Europe and the US are planning to belt and brace their border databases by using multiple forms of biometrics to identify people. While a set of fingerprints might be considered enough to tell one person from another, the trio expect to be eventually back this up with iris scans and mug shots. Frank Paul, head of large-scale IT systems at the European Commission’s directorate of Justice, Freedom and Security, said the move was necessary so the countries’ border systems could talk to one another. The trio have been trying to find a way to make their databases compatible so they can inform one another about suspected criminals and terrorists they want to catch and immigrants they want to keep out. But they have failed to co-ordinate their efforts so far. “There’ll never be a situation where the world will agree to have one biometric,” said Paul at a Homeland Security Conference in Brussels yesterday. “What we will have is a multi-modal environment.”

Source: The Register, June 28, 2007
http://www.theregister.co.uk/2007/06/27/multi-modal_border_biometrics/