



Strategic Policy & Cyber Media Research Division

**CYBER SECURITY INCIDENT
OUTSIDE MALAYSIA**

Report No. 17 – September 2008

15 September 2008

CyberSecurity Malaysia (726630-U)
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

DISCLAIMER	i
FRAUD	1
1. ICANN Cast As Online Scam Enabler	1
2. Scammers Skirt Spam Shields With Help From Adobe Flash	1
3. Carleton Collars Hacker	1
HACK THREAT/INTRUSION	2
4. Defending Islam, Hacker Defaces Thousands Of Dutch Websites.....	2
5. Hacker Attacks Police Website, Posts Anti-Graft Messages	2
6. 'Hacker Network' Targets UAE Banks In ATM Cash Fraud	3
7. 'Password Recovery' Services May Be Hackers For Hire	3
VIRUS/WORMS/TROJAN	4
8. Russian Spammers Involved In Building New Botnet For More Attacks..	4
9. Dramatic Rise In Botnet-Controlled PCs	4
10. USA Is Top Hosting Web-Based Malware Country	5
11. The Steady Rise Of Targeted Trojan Attacks	5
12. Facebook Application Herds PCs Into Botnet.....	5
13. Twitter Page Used To Pass Malware	6
14. New Tool Creates Fake YouTube Pages For Spreading Malware	6
15. 'UK's Chernobyl' Spam Spreads Trojan	6
SPAM	7
16. Get Heavy Spam, Blame Your Email ID	7
17. Spammers Use Free Web Services To Shield Harmful Links	7
OTHERS	8
18. Mother Of Israeli Hacker Held Over \$1.8m Fraud: FBI Framed	8
My Son	8
19. RAB Site Hacker Shahee Arrested.....	8
20. Companies Continue To Overlook Evolved Virus Attacks	9
21. Google, Police Take Cyber Crime Lessons To Schools	9
22. Hacker Gets Two Years For Stock Manipulation	10

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. ICANN CAST AS ONLINE SCAM ENABLER

Two recently issued reports portray the Internet Corporation for Assigned Names and Numbers (ICANN) as a bureaucracy that enables cyber criminals. In one report, researchers Jart Armin, James McQuaid and Matt Jonkman detail how one of ICANN's prized sponsors has ties to one of the net's more prolific sources of malware and illegal online pharmacies. It's called LogicBoxes, and over the past two years, ICANN has listed it as a sponsor for meetings that took place in Los Angeles and Delhi, India. It turns out that LogicBoxes has an association with Atrivo, a network provider that also goes by the name of Intercage. According to the study, a random sampling of 2,600 addresses hosted by Atrivo revealed 7,340 malicious web links, 910 infected websites, 310 malicious binaries, and 113 botnet command and control servers. As an autonomous systems (AS) provider, the Concord, California-based company controls a large number of IP addresses. The report details how Atrivo works with a rogue's gallery of other companies to enable anonymous sites that punt scareware, malware and online sites pushing Viagra and other sites. Other companies include Hostfresh, EstHost, EstDomains and PrivacyProtect.

Source: The Register, Sept 3, 2008

http://www.theregister.co.uk/2008/09/03/cyber_crime_reports/

2. SCAMMERS SKIRT SPAM SHIELDS WITH HELP FROM ADOBE FLASH

Online scammers have found a new way to skirt anti-spam filters, this time by making use of Adobe Flash files hosted on free websites. Spam messages with innocuous-looking content contain links to Flash-based files on ImageShack.com and elsewhere, according to a report from anti-spam service MessageLabs. Then commands embedded in the files redirect the recipient to sites that punt Viagra, work-at-home offers and free software updates. The technique allows spammers to bypass content filters employed by many anti-spam products, which immediately nix messages that contain links to dodgy sites. Because popular sites such as ImageShack are whitelisted, use of the Flash file allows spammers to bypass the filter but still lure marks to sites that try to bilk them or trick them into installing malware.

Source: The Register, Sept 4, 2008

http://www.theregister.co.uk/2008/09/04/spammers_using_adobe_flash/

3. CARLETON COLLARS HACKER

Carleton University, Canada, is questioning a student and will be taking disciplinary action after a hacker broke into the electronic accounts of 32 students. "He is cooperating with us. He has handed over his materials," said Chris Walters, a spokesman for the university. A math student, a man whose name has not been released, apparently hacked into the system to obtain password information of the students and then bragged to university

administration about it. Last week, a letter was sent to the university administration with a list of the accounts and their passwords. The writer claimed he easily broke into the accounts using a program that captures computer keystrokes and urged that the university improve security measures. The breach allowed for access to the Campus Cards that students use as debit cards for campus purchases, including photocopiers, food kiosks and the book store. None of the students reported missing money. With the information, the hacker could also have accessed e-mails, course registrations, library records and personal financial information about loans and scholarships.

Source: Computer Crime Research Centre, Sept 10, 2008

<http://www.crime-research.org/news/10.09.2008/3565/>

HACK THREAT/INTRUSION

4. DEFENDING ISLAM, HACKER DEFACTS THOUSANDS OF DUTCH WEBSITES

Over the last six weeks, a 'hacktivist' calling himself 'nEt^DeViL' has hijacked numerous Dutch sites, posting ideological statements on their home pages in retaliation for the anti-Islamic short film "Fitna" which was made and released earlier this year by a right-wing Dutch politician. Such an attack is known as website defacement. Zone-H.org, a website that tracks website defacement attacks worldwide, has documented thousands of compromised websites over the last months. Zone-H reports that 'nEt^DeViL' has hacked 18,157 websites as of Thursday, August 28.

Source: Department of Homeland Security, Sept 2, 2008

<http://www.itworld.com/security/54552/defending-islam-hacker-defaces-thousands-dutch-websites>

5. HACKER ATTACKS POLICE WEBSITE, POSTS ANTI-GRAFT MESSAGES

The Jakarta City Police's Traffic Management Center (TMC) website was the target of a hacking attack on Tuesday that lasted several hours. Information on Jakarta traffic was replaced with long messages criticizing the police. One of the messages read "The National Police was the third most corrupt organization in 2005, second most in 2006, and the most corrupt organization in 2007. Where is the justice? Today, all Indonesian Police websites are OWNED!" In the messages, the hacker, who claimed to have hacked all of the police's websites, said the next target would be the websites of Indonesian celebrities currently running for public office. "I don't know exactly why the hacker targeted the TMC. I think they chose it because it has many visitors, so more people would see the message, which was clearly aimed at ruining the police's image," TMC chief Comr. Sambodo Purnomo told The Jakarta Post. He said he suspected the hacker managed to infiltrate the website after the internet connection from state telecommunications company PT Telkom was temporarily disrupted. The website, www.lantas.metro.go.id, was defaced at dawn on Tuesday, returning to normal again at 1 p.m.

Source: Computer Crime Research Centre, Sept 10, 2008
<http://www.crime-research.org/news/10.09.2008/3564/>

6. 'HACKER NETWORK' TARGETS UAE BANKS IN ATM CASH FRAUD

Banks in the United Arab Emirates are struggling to resolve a security breach after it emerged that hackers used counterfeit bank and credit cards to steal funds from customers' accounts. The lenders declined to say how much money had been stolen or how many accounts were skimmed, but an initial investigation by the banks indicated that cash machines were rigged with devices that stole customers' PINs as they made withdrawals. Suvo Sarkar, general manager of retail banking for Emirates NBD, one of the nation's largest lenders, said: "We don't really know how this happened. However, one industry source suggested that the problem could be internal and more widespread. "The fact that the stolen numbers appear to have been stolen randomly suggests the banks themselves were somehow breached." Dubai Bank said that it had temporarily blocked international access to its cash machines after 42 of its customers' accounts were breached.

Source: Computer Crime Research Centre, Sept 12, 2008
<http://www.crime-research.org/news/12.09.2008/3568/>

7. 'PASSWORD RECOVERY' SERVICES MAY BE HACKERS FOR HIRE

Services that promise to help find lost passwords may make their living by cracking the passwords of others, says the chief security strategist at IBM's Internet Security Systems unit. Webmail services such as Gmail and Hotmail are widely used as a quick, low-cost alternative to more sophisticated email services offered by ISPs or corporations. But Webmail accounts are not particularly secure, he warns. For between \$300 to \$600, a hacker can find a full suite of Webmail cracking tools on the Internet, complete with the ability to do brute-force "guessing" of simple passwords and enhanced tools for penetrating the CAPTCHA authentication methods used on Webmail services, he notes. CAPTCHA-breaking methods have become so effective that for about \$100, the service provider can not only promise to give you the password to a specific Webmail account, but it can also promise to give you subsequent passwords if the legitimate owner should change passwords. There is not much that users can do to protect themselves from these hack-for-hire services, he says. "The best thing you can do is to use strong passwords," he says. It would be difficult for any company to set a policy against using Webmail services, he says. "Your best bet is to educate your users about the vulnerabilities of these services, and discourage them from using their Webmail accounts for transmitting company information or other sensitive data," he says. Users also should stay away from the services themselves, many of which are based in Russia or Southeast Asia and can be recognized by the stilted English grammar in their service descriptions, he notes.

Source: Department of Homeland Security, Sept 12, 2008
http://www.darkreading.com/document.asp?doc_id=163471&WT.svl=news1_1

VIRUS/WORMS/TROJAN

8. RUSSIAN SPAMMERS INVOLVED IN BUILDING NEW BOTNET FOR MORE ATTACKS

According to the University of Alabama at Birmingham (UAB) Spam Data Mine, the Russian-Georgian Cyber War reached a new height on the morning of August 17, 2008 when over 500 e-mails were received in just 90 minutes at the UAB. The university started receiving poorly crafted e-mails on August 15, 2008, and now they account for five percent of the total spam traffic. Moreover, the e-mails contain attractive headlines such as “Mikheil Saakashvili gay scam - news of the week” that lure victims into reading a phony BBC story on the Georgian President. The link provided in the e-mails takes victim to a web server loaded with malicious content and it tries to compromise the user’s system. It seems that spammers are trying to build a botnet but the motive behind establishing this network is still unclear. It may be used for launching more attacks against computers of the Georgian government. The director of Product Management with Symantec Security Response said that the malevolent software is a new variant of Trojan.Blusod program, as reported by NetworkWorld. Earlier, spammers used this Trojan to load antivirus program on computers by making users believe that their system infected with virus and the program could clean the problem on charges.

Source: Department of Homeland Security, Sept 3, 2008

<http://www.spamfighter.com/News-10882-Russian-Spammers-Involve-in-Building-New-Botnet-for-More-Attacks.htm>

9. DRAMATIC RISE IN BOTNET-CONTROLLED PCS

The number of computers currently controlled by botnets has exploded in recent months, according to researchers. Recent figures recorded by the Shadowserver Foundation reveal that the number of computers infected by botnets has quadrupled in the past 90 days. The increase comes despite a slight drop in the number of botnets, leading researchers to believe that the increase has largely benefited the established operators in the field. The increase has also come despite little to no increase in the volume of new malware and viruses being discovered in the wild. Some researchers believe that computers are being infected through web-based attacks, specifically SQL injection. A Sans Institute researcher noted that the increase in botnet infections seems to coincide with the appearance of large-scale SQL injection attacks, in which hundreds of thousands of web pages are compromised with embedded exploit code. He suggested that many security firms lack a mechanism for accurately rooting out the SQL attacks before they become widespread.

Source: Department of Homeland Security, Sept 4, 2008

<http://www.vnunet.com/vnunet/news/2225185/botnet-ranks-exploding>

10. USA IS TOP HOSTING WEB-BASED MALWARE COUNTRY

ScanSafe has issued data on the top three countries hosting Web-based malware including viruses, Trojans, root kits, password stealers, and other malicious programs. The U.S. ranked first (42 percent), China ranked second on the list (12 percent), and Germany ranked third (six percent). A large number of the malware hosts in the last month were part of the Asprox fast flux bot network—PCs that have been enlisted into the bot network and mask the true origin of the actual host. According to a ScanSafe report, web-based malware has already increased by 278 percent in the first half of 2008. Web users should not associate malware only with suspect websites. More and more legitimate sites are being targeted by attackers and websites where the Olympic Games are streamed online by broadcasters could be a prime area for compromise.

Source: Department of Homeland Security, Sept 4, 2008

http://www.securitypark.co.uk/security_article261940.html

11. THE STEADY RISE OF TARGETED TROJAN ATTACKS

Reports out of South Korea say that North Korean spyware made its way onto the computer of a South Korean army colonel. “A North Korean spyware e-mail was reportedly transmitted to the computer of a colonel at a field army command via China in early August. The e-mail contained a typical program designed automatically to steal stored files if the recipient opens it. It has not been confirmed whether military secrets were leaked as a result of the hacking attempt, but their scale could be devastating given that the recipient is in charge of the South Korean military’s central nervous system – Command, Control, Communication, Computer & Information (C4I).”

Source: Department of Homeland Security, Sept 5, 2008

http://www.informationweek.com/blog/main/archives/2008/09/the_steady_rise.html

12. FACEBOOK APPLICATION HERDS PCS INTO BOTNET

Researchers have created a proof-of-concept application for Facebook that turns the machines of people, who add the app to their Facebook page, into elements of a botnet. In a demonstration, the botnet launched denial-of-service attacks on a victim server. “Social-network websites have the ideal properties to become attack platforms,” according to the Antisocial Networks: Turning a Social Network into a Botnet paper, written by five researchers from the Institute of Computer Science in Greece and one researcher from the Institute for Infocomm Research in Singapore. The demo application, ‘Photo of the Day’, displays a new photo from National Geographic every day. However, every time someone views the photo, the host computer is forced “to serve a request of 600KB”, according to the paper. Such a botnet could be used for other types of attacks, such as spreading malware, scanning computers for open ports, and overriding authentication mechanisms that are based on cookies, the paper warns. The researchers suggested that Facebook and other social networks exercise caution in designing their platform and application programming interfaces (APIs) so that

there are few interactions between the “social utilities they operate and the rest of the internet”.

Source: Department of Homeland Security, Sept 9, 2008
<http://news.zdnet.co.uk/security/0,1000000189,39485526,00.htm>

13. TWITTER PAGE USED TO PASS MALWARE

In yet another new way to infect people, criminal hackers are using a Twitter page, according to one security researcher. In a blog, the director of malware research for Facetime explained how a Twitter page is being used to lure victims. To lend credibility to his discovery, the Twitter page lists 17 followers; however, each appeared to be fraudulent. The messages, written in Portuguese, attempt to get visitors to download a photo album. In order to view the album, you will need to download a Flash update, which is really the infection files themselves. The director and his team have identified the infection as Orkon. Once installed, the infected files do various things to the compromised desktop, such as attempt to gain your Orkut account log-in information, or displaying a browser image of a man identifying himself as the “Trickster.”

Source: Department of Homeland Security, Sept 10, 2008
http://news.cnet.com/8301-1009_3-10035580-83.html

14. NEW TOOL CREATES FAKE YOUTUBE PAGES FOR SPREADING MALWARE

Cyber criminals are getting more and more business-like. The latest examples involve a tool that automates the creation of fake YouTube web sites that can be used to deliver malware and password-cracking services for sale. Panda Security said it has uncovered a tool circulating in underground hacking forums, dubbed YTFakeCreator, that enables anyone to easily create a fake YouTube page that surreptitiously installs a Trojan, virus, or adware on a visitor's computer, said the chief corporate evangelist of Panda Security. The tool does not spread the video link on its own. An attacker must distribute it via e-mail, FTP, IRC channels, peer-to-peer file-sharing networks, or CD. Once a visitor arrives at the page, a fake error message appears saying that the video cannot be played because an important software component, such as a codec or Flash update, is missing. The visitor is prompted to download the software and the malware is installed. YTFakeCreator makes it easy for even unskilled people to set up an attack.

Source: Department of Homeland Security, Sept 15, 2008
http://news.cnet.com/8301-1009_3-10039974-83.html

15. ‘UK’S CHERNOBYL’ SPAM SPREADS TROJAN

A widespread spam campaign claims that a nuclear power plant on the outskirts of London exploded on Tuesday afternoon. The email claims to offer pictures of victims. In reality, the attached zip file is contaminated with a Trojan horse, identified by net security firm Sophos as Troj/Agent-HQE. Once the malware is

installed, hackers can use it to spy on the victim's computer and steal information for financial gain. The emails typically arrive with subject lines such as – Reply: A report on radiation contamination of Canada. “Rather than use a real life event, the hackers have turned to fictional explosions and conspiracy theories in the hope they will strike a nerve with potential victims who will then click on the attachment without a second thought,” commented a senior technology consultant at Sophos. “People are sometimes tempted to click on something they receive by email in the misguided belief that their anti-virus software will always protect them,” he added.

Source: Department of Homeland Security, Sept 15, 2008

http://www.theregister.co.uk/2008/09/11/chernobyl_uk_malware_ruse/

SPAM

16. GET HEAVY SPAM, BLAME YOUR EMAIL ID

How much spam you get depends on the first letter in your e-mail address, a Cambridge study reveals. Analysis of more than 500 million junk messages has found that addresses that began with more common letters were likely to receive 40 per cent of their mail from spammers. Those starting with less common letters, by contrast, would receive less than a fifth of their mail as spam. According to the study, if the first part of an email address (that part before the '@' symbol) starts with a J, A, U, I, R, P, M, or S, then it is likely to get proportionately twice as much junk email sent to it than an email address beginning with Q, Z, W, Y or F. Dr Richard Clayton, a computer scientist at Cambridge University who carried out the study, said he believed the difference could be explained by the first set of letters being more likely to appear at the start of names than the second set. The study did not draw a conclusion as to the exact cause of this phenomenon. However, Dr Clayton said there was some evidence to suggest that it could be due in part to the way some spammers launch 'Rumpelstiltskin' attacks. This is where the spammers use dictionary words and proper names in ascending alphabetical order in front of large numbers of domain names to generate their junk lists.

Source: Computer Crime Research Centre, Sept 8, 2008

<http://www.crime-research.org/news/08.09.2008/3562/>

17. SPAMMERS USE FREE WEB SERVICES TO SHIELD HARMFUL LINKS

Spammers are abusing free web services to make their spam links look more legitimate, according to e-mail security vendor MessageLabs Ltd. One of the services, a photo hosting site called ImageShack, lets people upload different types of photo formats, including Flash files, said a senior analyst at MessageLabs. Flash files, which have the extension “.swf,” can be used for animated graphics and to automatically redirect people to other Web sites — a feature that can be abused. The attack involving ImageShack works like this: Spammers upload a Flash file and then copy the link for that file, which comes from ImageShack's domain, into a spam message. If the link is followed, the

Flash file redirects the victim to a spam site, he said. The technique offers an advantage for spammers. Antispam software will often scan links in e-mail and block any e-mails with suspicious-looking links. But ImageShack's domain is considered to have a good reputation, so messages will not be blocked. Another, more dangerous variation on this theme is a spam e-mail promoting a video. If the link is clicked, a Flash file redirects the victim to a site where a pop-up window immediately implores the user to download a codec supposedly needed in order to play the video file. Invariably, the file is not a codec but rather some piece of malicious software.

Source: Department of Homeland Security, Sept 8, 2008

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9114045&taxonomyId=17&intsrc=kc_top

OTHERS

18. MOTHER OF ISRAELI HACKER HELD OVER \$1.8M FRAUD: FBI FRAMED MY SON

The mother of an Israeli living in Canada who has recently been arrested in Montreal on suspicion of committing fraud to the tune of \$1.8 million accused on Saturday the FBI of framing her son. "This is a conspiracy and the FBI is involved in it. A few U.S. bodies made it clear to Ehud that his day would come," said Ehud Tenenbaum's mother, Malka. "Ehud was never accused of stealing, he works hard at IT security and doesn't have to steal," she added. Canadian media reported on Friday that Alberta police suspect Ehud Tenenbaum and three co-conspirators hacked into the database of a Calgary financial services company. They then changed the value of the debit cards to an amount higher than their face value. The four suspects were arrested in Montreal and brought to Calgary on Tuesday. Tenenbaum has been charged with six counts of fraudulent use of credit card data and one count of fraud over \$5,000.

Source: Computer Crime Research Centre, Sept 8, 2008

<http://www.crime-research.org/news/08.09.2008/3560/>

19. RAB SITE HACKER SHAHEE ARRESTED

Bangladesh Rapid Action Battalion has arrested four people, including the RAB website hacker Shahee Mirza. Saboteurs hacked into the RAB website (www.rab.gov.bd) Friday night. RAB media cell director Abul Kalam Azad told bdnews24.com that they picked up four persons from a Mirpur residence Saturday night. The arrestees claimed they were students of a private institution. Shahee, 'leader' of the arrested youths, confessed to their hacking other sites belonging to different organisations. He also admitted the name and e-mail addresses he had posted after hacking the RAB site were real. Abul Kalam Azad said RAB would hold a press briefing at its headquarters later in the day. As people entered the website of the elite security force Friday night, they found the words 'Hacked by Shahee_Mirza' posted there. The hacker alleged that the

government had not taken sufficient steps for the development of IT in the country, though it had passed laws to prevent cyber crimes.

Source: Computer Crime Research Centre, Sept 8, 2008

<http://www.crime-research.org/news/08.09.2008/3561/>

20. COMPANIES CONTINUE TO OVERLOOK EVOLVED VIRUS ATTACKS

A recent security advisory from a messaging security company warned that service providers are placing e-mail users at risk by continuing to ignore sophisticated virus propagation techniques. Attackers are moving beyond traditional tactics, such as sending messages with virus executables attached or virus-infected documents, to employing hybrid attacks that combine elements of both spam and viruses. In these attacks, malware authors embed links in informative or advertising e-mails. Recipients are enticed to follow these links to a website that hosts the malware, which could be a virus, worm, or Trojan. These advanced threats embed anti-spam and anti-virus (AV) evasion techniques with the objective of eluding both spam and traditional AV filters. Most spam filters are not capable of catching these highly mutable threats because they do not follow the recurrent, mass e-mail tactics commonly found in spam. Likewise, conventional AV solutions bypass these messages as they appear to be spam or phishing. As these attacks become the norm, operators are urged to re-examine their anti-virus strategies and ensure that their messaging security processes are capable of detecting these hybrid threats.

Source: Department of Homeland Security, Sept 8, 2008

<http://www.govtech.com/gt/405320?topic=117671>

21. GOOGLE, POLICE TAKE CYBER CRIME LESSONS TO SCHOOLS

With youngsters becoming Internet savvy in the rapidly emerging world of computer technology, cyber crimes and misuse of Internet have also taken an upward curve. To help put a check on this, Google India, as a part of their BeNetSmart awareness initiative, carried out an awareness campaign in nine schools in Kolkata on Tuesday. “We decided to start a campaign to help students know how to avoid misuse of the internet and inculcate in them the best cyber practices,” said Rishi S Jaitly, policy analyst, Google India Pvt Ltd. The team interacted with 5,000 students in the city, added Jaitly. The nationwide programme first took off from Mumbai and Chennai after which it came to Kolkata. In this campaign, Kolkata Police assisted Google India in educating school students about proper internet usage. According to Jaitly, the Internet and Mobile Association of India, along with the police, are a part of this campaign.

Source: Computer Crime Research Centre, Sept 10, 2008

<http://www.crime-research.org/news/10.09.2008/3566/>

22. HACKER GETS TWO YEARS FOR STOCK MANIPULATION

A Malaysian hacker has been sentenced to two years in prison by US authorities for breaking into stock trading accounts and using them to ramp up prices in useless shares. Thirugnanam Ramanathan, 35, joined a group of hackers who bought low value shares from February to December 2006 then used stolen internet stock accounts to buy the same shares, thereby boosting the price. At least 60 customers and nine brokerage firms in the US have been identified as victims. According to information presented during the sentencing hearing, brokerage firms sustained more than \$300,000 in losses during Ramanathan's participation in the scam.

Source: Computer Crime Research Centre, Sept 12, 2008
<http://www.crime-research.org/news/12.09.2008/3570/>