

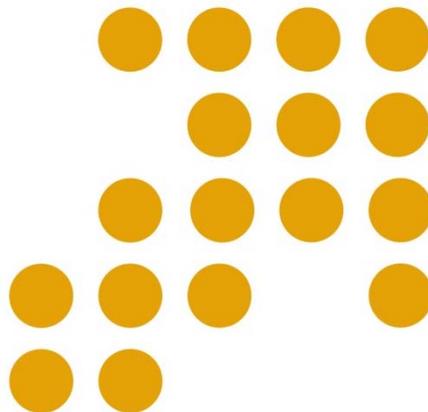


Cyber Security Policy Research Division

CYBER SECURITY INCIDENT OUTSIDE MALAYSIA

Report No. 8 – June 2010

16 June 2010



CyberSecurity Malaysia
Level 8, Block A,
Mines Waterfront Business Park
No 3, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan

Securing Our Cyberspace



An agency under
mosti
Ministry of Science,
Technology and Innovation

TABLE OF CONTENTS

DISCLAIMER	iii
1 FRAUD	1
1.1 420,000 SCAM EMAILS SENT EVERY HOUR	1
1.2 THE TRUTH ABOUT SOCIAL MEDIA IDENTITY THEFT.....	1
1.3 TIPS FOR PROTECTION AGAINST ONLINE IDENTITY THEFT.....	1
1.4 BIDEN TO FILE SHARERS: ‘PIRACY IS THEFT’.....	1
1.5 ELABORATE IDENTITY THEFT SCHEME TARGETS A MILLION CONSUMERS.....	2
2 HACK THREAT/INTRUSION	2
2.1 MAN INDICTED FOR HACKING AND THREATENING THE VICE PRESIDENT.....	2
2.2 IT PROS EXPECT NETWORK THREATS TO INCREASE AS BUDGETS DECLINE	3
2.3 ADOBE PATCHES PDF BUGS HACKERS ALREADY EXPLOITING.....	3
3 PHISHING ATTACK	3
3.1 FARMVILLE AND SEX AND THE CITY 2 USED FOR FACEBOOK CLICKJACKING	3
3.2 TEXT MESSAGE PHISHING ATTACKS DROP SIGNIFICANTLY	3
3.3 PHISHING REQUIRES MORE EFFORT THAN YOU MIGHT THINK	4
4 DOS.....	4
4.1 TELECOMMUNICATIONS DENIAL OF SERVICE ATTACKS.....	4
4.2 YOUTUBE USED TO SHOWCASE DDOS SOFTWARE	4
5 OTHERS.....	5
5.1 POOR PASSWORDS CAN LEAD TO DISASTER.....	5
5.2 MONTHS-OLD SKYPE VULNERABILITY EXPLOITED IN THE WILD.....	5

5.3 N.Y ATTORNEY GENERAL TACKLES CHILD PORN ON SOCIAL NETWORKS	5
5.4 HOW MUCH IS FACEBOOK DATA WORTH?.....	5
5.5 HOW CONSUMERS INFLUENCE DATA LOSS AND BREACHES.....	6
5.6 ERASING SENSITIVE INFORMATION FROM SMARTPHONES.....	.6
5.7 WHITE HOUSE DRAFTING PLAN FOR CYBERSPACE SAFETY.....	6
5.8 PROTECTION FOR THE ANDROID PLATFORM.....	7
5.9 FBI FAILS TO DECRYPT SUSPECT'S HARD DRIVES - AFTER 12 MONTHS OF TRYING	7
5.10 CISCO'S ACCESS POINT MIGRATION MODE LEAVES NETWORKS VULNERABLE.....	7

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.

1 FRAUD

1.1 420,000 SCAM EMAILS SENT EVERY HOUR

According to a report by CPP, more than 420,000 scam emails are sent every hour in the UK which estimates that Brits were targeted by 3.7 billion phishing emails in the last 12 months alone. A quarter of us admit to falling victim to e-fraudsters, with the average victim losing over GBP285 each. Fake banking emails are the most common method used by criminals, with 55 per cent of those targeted receiving seemingly legitimate e-correspondence from high street banks. Over half received false lottery or competition prize draws, while a further one in two was targeted by foreign cons such as the renowned "Nigerian 419 advance fee fraud" scam. Consumers must take caution, as latest industry figures show that online banking fraud rose by 14 per cent in the last 12 months. Fraudsters are also exploiting the explosion of social networking sites and current defaults in privacy settings to target victims.

Source: Help Net Security, June 16, 2010
<http://www.net-security.org/secworld.php?id=9421>

1.2 THE TRUTH ABOUT SOCIAL MEDIA IDENTITY THEFT

The use of social media can increase consumer vulnerability to identity theft because of the amount and type of personal information people share on these networks. However, according to a recent study by the Ponemon Institute, consumers do little or nothing to protect themselves. Although more than 80 percent of study respondents expressed concern about their security while using social media, more than half of these same individuals admitted they do not take any steps to actively protect themselves. Even though most respondents expressed concern about online security and privacy, nearly 90 percent did not feel

that identity theft is likely a risk from using social media sites. Accordingly, individuals continue to use social media despite acknowledged potential dangers.

Source: Help Net Security, June 21, 2010
<http://www.net-security.org/secworld.php?id=9445>

1.3 TIPS FOR PROTECTION AGAINST ONLINE IDENTITY THEFT

A recent study showed that while consumers recognize the importance of online privacy and security, most are not taking important protective measures to help guard their personal information. To help educate and inform social network users, ProtectMyID offers these tips for protection against online identity theft:

- Review and customize security settings.
- Review the privacy policy.
- Pick a password that can't be cracked.
- Log off when you leave.
- Install and update antivirus software.
- Make sure your wireless network connection is secure.

Source: Help Net Security, June 21, 2010
<http://www.net-security.org/secworld.php?id=9445>

1.4 BIDEN TO FILE SHARERS: 'PIRACY IS THEFT'

Do people commit theft when they share unauthorized copies of film and music over the Internet? U.S. Vice President Joe Biden thinks so. According to him, "Piracy is theft.

Clean and simple. It's smash and grab. It ain't any different than smashing a window at Tiffany's and grabbing [merchandise]." Biden spoke to the media alongside Victoria Espinel, the U.S. intellectual property enforcement coordinator, to introduce the government's strategy on protecting the country's intellectual property. Espinel also issued a report that included more than 33 recommendations, such as cooperating with foreign governments to go after foreign-based pirate sites.

Source: CNET News, June 22, 2010
http://news.cnet.com/8301-31001_3-20008432-261.html

1.5 ELABORATE IDENTITY THEFT SCHEME TARGETS A MILLION CONSUMERS

A federal court has halted an elaborate international scheme that used identity theft to place more than \$10 million in bogus charges on consumers' credit and debit cards, pending a trial. More than a million consumers were hit with one-time charges of \$10 or less, and their payments were routed through dummy corporations in the United States to bank accounts in Eastern Europe and Central Asia. According to the FTC complaint, the defendants, using phony company names resembling real companies, and information taken from identity theft victims in the United States, opened more than 100 merchant accounts with companies that process charges to consumers' credit and debit card accounts. The FTC believes the defendants may have run credit checks on the identity theft victims first, to be sure they were creditworthy. The defendants also cloaked each fake merchant with a virtual office address near a real merchant's location, a phone number, a home phone number for the "owner," a Web site pretending to sell products, a toll-free number consumers could call, and a real company's tax number found on the Internet.

Source: Help Net Security, June 29, 2010

<http://www.net-security.org/secworld.php?id=9495>

2 HACK THREAT / INTRUSION

2.1 MAN INDICTED FOR HACKING AND THREATENING THE VICE PRESIDENT

A 45-year-old Blaine, Minnesota man has been indicted in federal court in the District of Minnesota for hacking into his neighbor's wireless Internet system and allegedly posing as the neighbor to make threats to kill the vice president of the United States and. The indictment alleges that in February 2009, Ardolf hacked into his neighbor's wireless Internet connection and created multiple Yahoo.com e-mail accounts in that person's name. Ardolf allegedly signed the e-mail with the name of the neighbor as well as the name of the person's wife. The indictment alleges that Ardolf sent the e-mail using the wireless router belonging to the neighbor, intending for the e-mail to be traced back to that person. In February 2009, Ardolf posed as the identity-theft victim and used the e-mail accounts he created in the victim's name to send sexually themed e-mails to three of the victim's co-workers. In one of the e-mails, Ardolf attached an image containing child pornography. Ardolf also allegedly created a MySpace page in the victim's name, on which he posted the same image of child pornography. If convicted, Ardolf faces a potential maximum penalty of 20 years in prison on the distribution of child pornography charge, 10 years on the pornography possession charge, five years on both the unauthorized access to a computer and the threats to the vice president, and a mandatory two-year minimum prison sentence on each count of aggravated identity theft.

Source: Help Net Security, June 24, 2010
<http://www.net-security.org/secworld.php?id=9475>

2.2 IT PROS EXPECT NETWORK THREATS TO INCREASE AS BUDGETS DECLINE

Of the 100-plus netForensics survey respondents, 85% believe their organization's security environment will grow more complex over the next 24 months, leading to additional security threats in the second half of 2010 and into 2011. Yet, 53% believe their organization is not budgeting enough on security to manage increasing threats. According to Dale Cline, CEO of netForensics, based on the findings of their study, organizations are cutting security staff to reduce costs, yet the overall perception is that organizations will ultimately face more threats this year and next. With security staff remaining static or decreasing, and budgets not being allocated to put security processes in place, organizations are going to face greater challenges than ever to their security posture.

Source: Help Net Security, June 24, 2010
<http://www.net-security.org/secworld.php?id=9471>

2.3 ADOBE PATCHES PDF BUGS HACKERS ALREADY EXPLOITING

Adobe on Tuesday patched 17 critical vulnerabilities in Reader and Acrobat, including one that hackers have been using for nearly a month to commandeer PCs. Another patch fixed a design flaw in the PDF format that attackers have been exploiting since April to dupe users into downloading a Trojan horse. Adobe rushed the security update, which was originally slated to ship July 13, because exploit code went public and attacks using rigged PDF documents started showing on antivirus vendors' reporting systems four weeks ago. The company patched Flash -- hackers were tricking people into visiting malicious

sites, then using the same bug to launch drive-by attacks on June 10.

Source: Computerworld News, June 30, 2010
http://www.computerworld.com/s/article/9178740/Adobe_patches_PDF_bugs_hackers_already_exploiting

3 PHISHING ATTACK

3.1 FARMVILLE AND SEX AND THE CITY 2 USED FOR FACEBOOK CLICKJACKING

PandaLabs reported the proliferation of scams hijacking the Facebook "Like" option. The attack uses eye-catching messages related to the popular game Farmville or the Sex and the City 2 movie to grab the attention of logged-in Facebook users as they browse web pages with the "Like" button, the Facebook wall feature or messaging system. This technique, known as clickjacking, uses a simple application to launch a Javascript action. Visiting users are tricked into liking a page without necessarily realizing that they are recommending it to all of their Facebook friends. The real business stems from the pay-per-click system, which counts every click and generates revenue for affiliates, and from the tests offered to users on every page, which they must pay to make.

Source: Help Net Security News, June 16, 2010
<http://www.net-security.org/secworld.php?id=9423>

3.2 TEXT MESSAGE PHISHING ATTACKS DROP SIGNIFICANTLY

According to a report by Internet Identity (IID), text-to-phone phishing attacks (often called "smishing") dropped dramatically in the first quarter of 2010. Smishing attacks were down 62 percent from January to March, 2010, compared to the previous quarter. Despite the drop, the number of

credit unions being impersonated in text-to-phone cases stayed the same, meaning these organizations were the most targeted by industry. In these attacks, cyber criminals impersonated companies by text message to try and lure victims to call a fake interactive voice response (IVR) system designed to steal vital personal data like logon information, account credentials, social security numbers and more.

Source: Help Net Security, June 17, 2010
<http://www.net-security.org/secworld.php?id=9432>

3.3 PHISHING REQUIRES MORE EFFORT THAN YOU MIGHT THINK

When it comes to setting up phishing pages, there are some phishers that make the extra effort. Take those behind the fake Orkut login pages, for example. Symantec has been following their work, and noticed that phishers make the same changes to the websites that the original site makes namely, the logo that change on special occasions such as Earth Day, Mother's Day, and others. Google had actually a pretty good idea with this logo-changing practice: not only it makes the services look more friendly and reminds the users that the sites are constantly monitored and updated, but it also makes "lazy" phishers fail.

Source: Help Net Security, June 24, 2010
<http://www.net-security.org/secworld.php?id=9472>

4 DOS

4.1 TELECOMMUNICATIONS DENIAL OF SERVICE ATTACKS

The FBI released a warning to consumers concerning a new scheme using telecommunications Denial of Service (TDoS) attacks. The FBI determined fraudsters compromised victim accounts

and contacted financial institutions to change the victim profile information (i.e. email addresses, telephone numbers and bank account numbers). The TDoS attacks used automated dialing programs and multiple accounts to overwhelm victims' cell phones and land lines with thousands of calls. When victims answered the calls they heard dead air (nothing on the other end), an innocuous recorded message, advertisement, or a telephone menu. Calls were typically short in duration but so numerous that victims changed their phone numbers to terminate the attack. These TDoS attacks were used as a diversion to prevent financial and brokerage institutions from verifying victim account changes and transactions. Fraudsters are afforded adequate time to transfer funds from victim brokerage and financial online accounts.

Source: Help Net Security, June 21, 2010
<http://www.net-security.org/secworld.php?id=9446>

4.2 YOUTUBE USED TO SHOWCASE DDOS SOFTWARE

Facebook, Twitter and YouTube accounts are becoming the norm and a must for a successful business, but it would be erroneous to think that only legitimate businesses can take advantage of them. Advertising their wares on underground forum is how criminals usually try to sell their illegal wares, but Trend Micro has recently discovered an instance where criminals availed themselves of the possibility to post a video on YouTube in order to showcase how their DDoS tool works. The video has since been taken down by YouTube, but not before the researchers were able to notice that the price (\$15) and the URL where the tool can be bought were listed, and that the video has been viewed more than 600 times.

Source: Help Net Security, June 28, 2010
<http://www.net-security.org/secworld.php?id=9488>

5 OTHERS

5.1 POOR PASSWORDS CAN LEAD TO DISASTER

Passwords are valuable information and when they fall in the wrong hands, the end result can be a personal and financial disaster. Many people have established secure password habits but a surprisingly large number still rely on just one password for all their needs. According to a survey by F-Secure, about 20% of Internet users in Germany, Sweden and the UK use the same passwords for everything – from credit cards to online banking to logging into their e-mail account or a game website. About 20% write their password on a piece of paper, while 8% have to reset their passwords frequently because they forget them so easily. Another F-Secure survey conducted in seven countries reveals that, on average, only about 50% of mobile phone users protect their phones with a password. According to the survey, Germans are the most security conscious with 68% locking their phones with passwords, while the British (27%) and Americans (13%) lag far behind in terms of safe mobile phone use. Sean Sullivan, Security Advisor at F-Secure, says, "With so many logins to deal with these days, it is tempting to use just one or two passwords for everything. Unfortunately it is also a recipe for disaster because there is a whole industry of cybercriminals constantly devising new ways to steal passwords and exploiting them to the full."

Source: Help Net Security, June 16, 2010
<http://www.net-security.org/secworld.php?id=9420>

5.2 MONTHS-OLD SKYPE VULNERABILITY EXPLOITED IN THE WILD

A Skype flaw patched some 9 months ago with the new version (4.1.0.179) of the VoIP client has been spotted being exploited in

the wild. According to M86 Security Labs, the vulnerability has been discovered in the EasyBits Extras Manager, a plug-in component for Skype, and for all those people who haven't updated their client, this presents a gaping hole in their security perimeter. Bradley Anstis, VP of Technology for M86 Security says that there is no evidence that the campaign is a massive one, but it definitely points out the fact that updating software is of crucial importance.

Source: Help Net Security, June 17, 2010
<http://www.net-security.org/secworld.php?id=9429>

5.3 N.Y ATTORNEY GENERAL TACKLES CHILD PORN ON SOCIAL NETWORKS

New York Attorney General, Andrew Cuomo has spearheaded the creation of a database of "digital fingerprints" to flag child pornography and keep it off from social networks. With the hash values of over 8,000 known child-porn images stored in the database, Cuomo said that he hopes its intended clients like social-networking, file-sharing, and photo-storage sites will start to use it "immediately." Here's how it works: the collection of "digital fingerprints," compiled through law enforcement efforts over the years, can be used as a filter by a partner social network. So when a photo is uploaded, it can be checked against the contents of the database. If there's a match, the photo is not permitted to be uploaded. Use of the database is also available to law enforcement authorities.

Source: CNET News, June 17, 2010
http://news.cnet.com/8301-13577_3-20008079-36.html

5.4 HOW MUCH IS FACEBOOK DATA WORTH?

Facebook has over 400 million active users. Can you even imagine how much freely

given, highly accurate user data is stored on each of those accounts? The benefits of Facebook lay in the fact that you can stay in touch with friends and family, meet new people and play a few games, but to the aforementioned interested parties, the information you provide is a clear route to your wallet. According to PC World, SharesPost estimates the value of Facebook at around \$11.5 billion. Advertisers and marketers are rubbing their palms together in satisfaction at the thought of having access to carefully selected groups of users that are formed by analyzing demographic and psychographic information. Last but not least, we have the criminals. Technical flaws and social engineering, worms and phishing attacks are used by malicious individuals to break into your account, access the information in it and use it to perpetrate identity theft.

Source: Help Net Security, June 22, 2010
<http://www.net-security.org/secworld.php?id=9429>

5.5 HOW CONSUMERS INFLUENCE DATA LOSS AND BREACHES

Cisco announced the results of a survey exploring the security implications of social networking and the use of personal devices in the enterprise. One of the most striking findings was that employees are consistently working around information technology security policies to use unsupported devices and applications. Another significant finding, 71 percent of the survey respondents said that overly strict security policies have a negative impact on hiring and retaining employees under age 30. The survey polled 500 IT security professionals across the United States, Germany, Japan, China and India. The results illustrate that the consumer influence on enterprise IT is growing and that more employees are bringing personal devices and applications into the network,

presenting new business opportunities and security challenges.

Source: Help Net Security, June 24, 2010
<http://www.net-security.org/secworld.php?id=9470>

5.6 ERASING SENSITIVE INFORMATION FROM SMARTPHONES

With increasingly faster mobile networks, users of both personal and business smartphones often have easy access to company applications that contain sensitive information. While organizations frequently provide access to company messaging and folder systems via smartphones, they overlook the danger of data breach when the device is retired. Blancco Mobile Edition is designed to eliminate the risk of inadvertent data leaks by erasing retired smartphones that may contain both sensitive business and personal information. Capable of erasing up to 150 such devices per day, the software helps IT security managers set and enforce end-of-service policy related to smartphones.

Source: Help Net Security, June 28, 2010
<http://www.net-security.org/secworld.php?id=9485>

5.7 WHITE HOUSE DRAFTING PLAN FOR CYBERSPACE SAFETY

The White House is hoping to come up with a comprehensive strategy to better protect people in cyberspace and is asking the public for help. Releasing a draft of the potential new National Strategy for Trusted Identities in Cyberspace last Friday, the government is aiming to set up a system that would let people voluntarily create trusted identities to use in online transactions. The goal, as described in a blog post by White House cybersecurity chief Howard Schmidt, is to secure and protect transactions in cyberspace through use of a special ID, a smart card or digital

certificate that would prove that people are who they say they are. These digital IDs would be offered to consumers by online vendors for financial transactions. Looking for suggestions from the public, the U.S. Department of Homeland Security has launched a Web site to elicit ideas and feedback on the NSTIC. The government plans to collect comments at the site through July 19 before promising to finalize its strategy later this fall.

Source: CNET News, June 24, 2010
http://news.cnet.com/8301-13578_3-20008998-38.html

5.8 PROTECTION FOR THE ANDROID PLATFORM

F-Secure Mobile Security 6 on the Android platform has been released. It provides security for smartphones against malicious software and also safeguards confidential data even if the phone is lost or stolen. Browsing Protection identifies which websites are safe to enter and blocks harmful sites that try to spread malware or steal confidential information, such as banking details. The Anti-Theft feature makes it possible to remotely lock the phone or erase the data on the phone if it is lost or stolen. It can also inform you of the new number if the SIM card is changed and show you the phone's location, so you can track down who has your smartphone.

Source: Help Net Security, June 29, 2010
<http://www.net-security.org/secworld.php?id=9491>

5.9 FBI FAILS TO DECRYPT SUSPECT'S HARD DRIVES- AFTER 12 MONTHS OF TRYING

After 12 months of failed attempts to crack the encryption that protects information held on five hard drives that belong to a Brazilian banker suspected of money laundering, the FBI has returned the drives to the experts of the Brazilian National Institute of Criminology (INC). The contents of the

drives protected by a combined use of TrueCrypt (free open-source full-disk encryption software) and an unnamed algorithm though to be base on the 256-bit AES standard are still a mystery. Both the INC and the FBI tried for months to break the encryption by using various dictionary-based brute-force attacks, since there is no law in Brazil that could be used to compel the suspect banker or the TrueCrypt Foundation to give up the access codes to the discs. According to The Register, this unusual case illustrates beautifully "how care in choosing secure (hard-to-guess) passwords and applying encryption techniques to avoid leaving file fragments that could aid code breakers are more important in maintaining security than the algorithm a code maker chooses."

Source: Help Net Security, June 30, 2010
<http://www.net-security.org/secworld.php?id=9506>

5.10 CISCO'S ACCESS POINT MIGRATION MODE LEAVES NETWORKS VULNERABLE

A feature of Cisco's Aironet 1200 Series Access Point can be abused by hackers to gain access to a company network, claim researchers from Core Security Technologies. The device is usually used to power wireless LANs, and has the option of being set to a WPA migration mode, in order to allow companies to gradually migrate from using the insecure WEP encryption, using more secure WPA standard without having to upgrade the equipment all at once. If this migration mode is not disabled after the migration is complete, the network is as insecure as it was before when WEP devices were used, since the researchers managed to crack the network encryption key by forcing the device to send out WEP broadcast packets.

Source: Help Net Security, June 30, 2010
<http://www.net-security.org/secworld.php?id=9503>