



Cyber Security Policy Research Division

CYBER SECURITY INCIDENT OUTSIDE MALAYSIA

Report No. 9 – June 2010

1 July 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 ELDERLY COUPLE SENT \$512,000 TO OVERSEAS SCAMMERS.....	1
1.2 IT STAFFER AT NEW YORK BANK PLEADS GUILTY TO DATA THEFT, FRAUD.....	1
1.3 WHEN IDENTITY THEFT IS NOT YOUR FAULT.....	1
1.4 SCAMMERS TARGETING FAMILIES OF U.S. SOLDIERS IN IRAQ	2
2 HACK THREAT/INTRUSION	2
2.1 10,000 XP MACHINES ATTACKED THROUGH 0-DAY FLAW.....	2
2.2 YOUTUBE HACK: NO VIRUS, JUST A XSS FLAW AND IT'S ALREADY FIXED	2
2.3 12 MONTHS IN PRISON FOR HACKING.....	3
2.4 THE PIRATE BAY HACKED, USER INFORMATION EXPOSED.....	3
2.5 U.S. SENATOR'S EMAIL HACKED AND USED TO SENT OUT SCAM EMAILS.....	3
2.6 FACEBOOK FOR HACKERS SHUT DOWN IN PAKISTAN.....	4
3 PHISHING ATTACK	4
3.1 FACEBOOK CREDENTIALS PHISHING SCHEME.....	4
3.2 TAX CREDITS FILING DEADLINE PHISHING ATTACKS	4
4 SPAM	5
4.1 TWITTER KIT, A SPAMMER'S DREAM COME TRUE	5
5 OTHERS.....	5
5.1 ONLINE CRIMES NOT JUST 'SPECCY GEEKS', RESEARCHERS WARN	5
5.2 MOST CYBER ATTACKS TARGET THE U.S.....	5
5.3 RISK OF CYBER THREATS SERIOUSLY UNDERESTIMATED.....	6

5.4 HOUSE VOTES TO BLOCK NET PORN ON GOVERNMENT PCS 6
5.5 FACEBOOK TO PROMOTE NEW U.K. SAFETY APPLICATION 6
**5.6 CYBERCRIMINALS INCREASE EFFECTIVENESS WITH MULTI-STAGE
ATTACKS 6**
5.7 WHITE HOUSE DRAFTING PLAN FOR CYBERSPACE SAFETY.....6

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 ELDERLY COUPLE SENT \$512,000 TO OVERSEAS SCAMMERS

In the Australian Transaction Reports and Analysis Centre's annual report on crime typologies and case studies, there is a particular one that caught the author's attention. The case of an elderly couple that have been duped into sending money to various people all over the world and continued to do it even after they were being warned by the police that it is highly likely, these recipients were international fraudsters. On four separate occasions, the couple has sent money to people in Africa, UK and Hong Kong, and they lost a little over half a million of Australian dollars in total. The fraudsters based in the UK and in Hong Kong carried out an "inheritance" scam, while the Ghana and Ivory Coast-based scammers as it happens, two women forged a friendly relationship with the couple over the Internet and asked for (and received) money for food, accommodation and other expenses. The husband even traveled to Ghana on one occasion and met the woman. Law enforcement officers visited the couple in relation to the money transfers connected to these four recipients and talked to them about the high probability that these recipients were scammers, but have obviously not made much of an impact, since the couple continued to send money overseas.

Source: Help Net Security, July 1, 2010
<http://www.net-security.org/secworld.php?id=9514>

1.2 IT STAFFER AT NEW YORK BANK PLEADS GUILTY TO DATA THEFT, FRAUD

A former IT staffer with the Bank of New York Mellon pleaded guilty for stealing sensitive information belonging to 2,000 bank employees and then using that data to

steal more than \$1 million from charities. He pleaded guilty to theft, money laundering and computer tampering charges in New York City Criminal Court Thursday. According to the district attorney's office in its press release, over an eight-year period, Adeyemi stole more than \$1.1 million from charities by transferring funds from the charities' bank accounts into bogus accounts he had set up using the personal information of his former co-workers. He "input the charities' banking details, including account and routing numbers, to set up wire transfers on the E*Trade and Fidelity sites from the charities' account to his dummy accounts, and withdrew the stolen funds or transferred them to a second layer of dummy accounts. He also spent the proceeds on U.S. Postal Service money orders, to pay his rent and credit cards, and to purchase goods that were then shipped to Nigeria.

Source: Computerworld, July 3, 2010
http://www.computerworld.com/s/article/9178840/IT_staffer_at_New_York_bank_pleads_guilty_to_data_theft_fraud

1.3 WHEN IDENTITY THEFT IS NOT YOUR FAULT

It is definitely true that you should be responsible for the security of your information when you handle it, but what happens when the theft of your information is not your fault? You have handed over this information to a company or organization and trusted them to keep it secure, but they failed. They might notify you of the breach or theft, and they might even set up a credit monitoring service for you for a year or two, but the problem is that this information may be used years from now. Is it fair that you have to worry for decades and pay for further credit monitoring when they are to blame for your information ending up in the wrong hands? Individuals whose information has been stolen have probably asked these questions over and over again. Take Jake McCoy as an example. He has applied for loans in

order to pay for his education, and is still paying them back. Two years ago, he was notified by his Alma Mater that a laptop containing his account information has gone missing. According to CNN, they apologized and arranged for a one-year long credit monitoring service, which has since expired. Unfortunately for him and 350 million people whose personal records have been compromised by data privacy breaches since 2005, there is not much he can do apart from paying for the credit monitoring service in the years to come. Companies are encouraged to use encryption to secure this and other kinds of sensitive data, but they often don't do it. Encryption slows down their day-to-day operation and that means extra cost. But the Data Accountability and Trust Act that will soon be voted on by the U.S. Senate may change the situation for the affected customers for the better. If the Act is confirmed, the companies will be compelled to take "reasonable measures" to protect data containing personal information.

Source: Help Net Security, July 12, 2010
<http://www.net-security.org/secworld.php?id=9559>

1.4 SCAMMERS TARGETING FAMILIES OF U.S. SOLDIERS IN IRAQ

If you receive an email or a Facebook message apparently coming from Ray Odierno, Commanding General of the United States Forces in Iraq, offering to get your loved one out of harm's way (i.e. home) in exchange for the exorbitant sum of \$200,000 just delete it. The New York Times reports that the General has recently acknowledged that his name is being (mis)used in different online scams. One even tried to fool recipients into believing that he was looking for their help to move out a "hidden" treasure from Iraq.

Source: Help Net Security, July 13, 2010
<http://www.net-security.org/secworld.php?id=9569>

2 HACK THREAT / INTRUSION

2.1 10,000 XP MACHINES ATTACKED THROUGH 0-DAY FLAW

The Windows Help and Support Center vulnerability, the details of which have recently been made public by researcher Tavis Ormandy, is being heavily exploited in the wild. According to a recent post on Microsoft's Malware Protection Center Blog, public exploitation of the vulnerability started on June 15th, but those attacks were probably undertaken by other researchers, since they were targeted and rather limited. Microsoft claims, over 10,000 separate computers have reported witnessing this attack. Computers in Portugal and Russia have seen by far the highest concentration of attacks. The attacks only increased with time. Microsoft started seeing "seemingly-automated, randomly-generated HTML and PHP pages hosting this exploit", and the goal of the attacks was to plant Trojans and viruses on the targeted system.

Source: Help Net Security, July 1, 2010
<http://www.net-security.org/secworld.php?id=9515>

2.2 YOUTUBE HACK: NO VIRUS, JUST A XSS FLAW AND IT'S ALREADY FIXED

This Independence Day weekend seemed like the perfect time for hackers to take advantage of a cross-site scripting vulnerability in YouTube's comments to bombard the users with annoying pop-ups that often contained fake news of a deadly car crash that involved teen star Justin Bieber and links that would take them to adult-content sites. The hackers even managed to disable comments altogether. The hackers managed to bypass the filter that sanitizes the HTML code employed in the comments, and insert their own scripts. The attack was extremely simple to execute two script tags in a row allowed the hackers

to insert Javascript in the comments. According to Google spokesman, luckily for the users, YouTube reacted promptly. Comments were temporarily hidden by default within an hour, and they released a complete fix for the issue in about two hours.

Source: Help Net Security, July 5, 2010
<http://www.net-security.org/secworld.php?id=9530>

2.3 12 MONTHS IN PRISON FOR HACKING

A former senior database administrator for GEXA Energy in Houston was sentenced to 12 months in prison for hacking into his former employer's computer network. Steven Jinwoo Kim, 40, of Houston pleaded guilty on Nov. 16, 2009, to one count of intentionally accessing a protected computer without authorization and recklessly causing damage. Kim was ordered to pay \$100,000 in restitution to GEXA Energy and to serve three years of supervised release following his prison term. In pleading guilty, Kim admitted that in the early hours of April 30, 2008, he used his home computer to connect to the GEXA Energy computer network and a database that contained information on approximately 150,000 GEXA Energy customers. While connected to the computer network, Kim recklessly caused damage to the computer network and the customer database by inputting various Oracle database commands. Kim also copied and saved to his home computer database file containing personal information on the GEXA Energy customers, including names, billing addresses, social security numbers, dates of birth and drivers' license numbers.

Source: Computerworld News, July 7, 2010
<http://www.net-security.org/secworld.php?id=9543>

2.4 THE PIRATE BAY HACKED, USER INFORMATION EXPOSED

It is one problem after another for the (in) famous file-sharing Web site. Dogged by the music and movie industry, its founders are defending themselves and their creation in the court of law and the site is in danger of getting its domain seized by the US Government. A group of Argentinian hackers (or, as they call themselves, security researchers) has discovered multiple SQL injection vulnerabilities that allowed them to access the site's administration panel and, through it, information regarding its members' usernames, e-mail and IP addresses, the number and name of torrents uploaded by users, and other data could be viewed, modified or deleted by the group, although they claim that they did not alter or delete any of it. As they told Brian Krebs, their goal was to show to the users that their information is not adequately protected. Krebs received confirmation of the hack when he shared his TPB username with Russo, and Russo reciprocated by sending him the matching e-mail address and a hash of the password. Russo says that the site administrators seem to have already patched the vulnerabilities, although administrators have yet to offer a comment on the situation.

Source: Help Net Security, July 8, 2010
<http://www.net-security.org/secworld.php?id=9552>

2.5 U.S. SENATOR'S EMAIL HACKED AND USED TO SENT OUT SCAM EMAILS

According to Softpedia reports, the Yahoo email account of Bob Dvorsky, Iowa State Senator, has been compromised by unknown individuals who used it to send a variation of the "friend in need" scam email to his contacts. The email contained an emergency message telling that he misplaced his wallet during a trip to Scotland and would like to assist him with a

loan of 10,000 Pounds to sort his hotel bills and to get back home. The idea that a U.S. Senator can be stuck in a foreign country because he lost his wallet is just laughable. According to an interview given to KCRG-TV9, the Senator says that he is fairly sure that his email password was stolen a couple of months ago, when he received an email claiming to be from a representative of Yahoo and asking for his password. He believed the email to be legitimate and shared his password with the scammers that ultimately hijacking the account. Other politicians have also not been so lucky. When email accounts of Alaska Governor Sarah Palin and South Carolina Governor Mark Sanford were compromised, their contents were made public.

Source: Help Net Security, July 9, 2010
<http://www.net-security.org/secworld.php?id=9557>

2.6 FACEBOOK FOR HACKERS SHUT DOWN IN PAKISTAN

Five alleged hackers have been arrested by the Pakistani authorities in raids that led to the closure the Pakbugs hacking and carding forum. The operation, run by Pakistan's Cyber Crime department of Federal Investigation Agency (FIA), followed complaints by "national and multinational organisations" over a series of website defacement and hack attacks. Pakbugs is blamed for running amok across thousands of websites belonging to various governmental and non-governmental organisations in Pakistan and elsewhere, local telecoms blog PakSpider reports. A Pakistani government press statement explains that the suspects are thought to have expertise in a range of cybercrime techniques, including botnet management, phishing and carding. F-Secure added that Pakbugs.com was a full service cybercrime forum that offered a venue to discuss hacking techniques and a marketplace for the sale malware code, bank logins and stolen credit card numbers. Last year someone hacked into the forum and posted

confidential information to a Full Disclosure mailing list. The information posted included logins, email addresses and password hashes, the Finnish net security firm adds.

Source: The Register, July 13, 2010
http://www.theregister.co.uk/2010/07/13/pakbug_s_crackdown/

3 PHISHING ATTACK

3.1 FACEBOOK CREDENTIALS PHISHING SCHEME

Trying to trick users into giving up their Facebook usernames (i.e. emails) and passwords by making them believe they have won a prize is a well-known tactic employed by online criminals. Sunbelt's Chris Boyd encountered this particular one while he was trying to access a legitimate application on Facebook. Out of curiosity, he clicked on the green check button and, sure enough, the user is required to give up his or hers account data in order to claim the "winnings". Boyd followed pop-up window the day after in order to see if Facebook had done something about the scheme and they did. The link has been redirected to a warning page that advises users who have fallen for the scheme to reset their account password.

Source: Help Net Security, July 2, 2010
<http://www.net-security.org/secworld.php?id=9522>

3.2 TAX CREDITS FILING DEADLINE PHISHING ATTACKS

July 31st is the deadline to file a tax credits renewal with HMRC or pay the second installment of income tax. The danger now, says Trusteer, is that tax credit filers will click on unsolicited emails that look as though they might have been sent by HMRC, and in doing so, may end up infecting their home or office computers. "Back in February we warned online

banking users of phishing and malware infections stemming from emails offering Internet users a tax refund. And given that such phishing emails are twice as successful as bank phishing attacks, cybercriminals have realized that an email with HMRC in its message header is a lot more attractive to recipients," said Mickey Boodaei, Trusteer's CEO. It is likely that hackers will exploit this interest in tax credits and tax refunds generally, with a rash of infected emails and/or messages with links to infected web sites.

Source: Help Net Security, July 7, 2010
<http://www.net-security.org/secworld.php?id=9541>

4 SPAM

4.1 TWITTER KIT, A SPAMMER'S DREAM COME TRUE

Cyber criminals and spammers have been misusing Twitter for a long time. Twitter has tried to stop or at least limit their use of the platform by defining some web page limitations regarding the amount of messages and updates allowed per day or per hour, and other things like API requests and changes of the email account. Unfortunately for Twitter, the fight against these spammers is often similar to a game of Whack-A-Mole that takes a malicious account down, another spring up in its place. Finding a way to bypass the limitations set by the social network is another key to success for these malicious users. Trend Micro has recently spotted a toolkit being offered for sale on many underground forums. Dubbed "Twitter Kit", it allows the malicious user to send messages to thousands of followers using SOCKS5 proxy and to send *Follow* invites to users and their followers. It also breaks the aforementioned account limits set by the social network.

Source: Help Net Security, July 5, 2010
<http://www.net-security.org/secworld.php?id=9528>

5 OTHERS

5.1 ONLINE CRIMES NOT JUST 'SPECY GEEKS', RESEARCHERS WARN

Misconceptions about the nature of cybercrime are affecting the fight against online economic skullduggery. According to researchers from Trend Micro, which reckons the majority of cyber crooks would be indistinguishable from the man in the street, widespread beliefs that e-crooks are likely to be either "geeks with glasses" or digital pranksters are well wide of the mark. Cyber gangs are located around the world. Russia, the Ukraine and China are well known havens for hackers, helped by the difficulty of getting foreign complaints against economic crime to local law enforcement taken seriously. Other countries including Turkey, Brazil and Estonia also commonly crop up as the home of hackers in cybercrime investigations. Since cybercrime is global, the only effective way to tackle this crime is to enforce collaboration across law enforcement agencies in different countries and continents, Trend Micro argues. However, international co-operation is frustrated by the fact many police forces often intervene only when there's enough evidence to suggest there is a single entity that happens to be located within their jurisdiction behind criminal activity.

Source: The Register, July 1, 2010
http://www.theregister.co.uk/2010/07/01/cybercrime_gang_profile/

5.2 MOST CYBER ATTACKS TARGET THE U.S.

SecureWorks announced the findings of a research study that analyzed where the greatest number of attempted cyber attacks were launching from across the globe at its 2,800 clients. India won the study by having the lowest number of attempted cyber attacks originating from computers within its

borders with only 52 attacks per thousand PCs. The Netherlands ended in second place with 57 attacks per thousand PCs, narrowly beating Germany and Brazil who came in third and fourth place respectively. The UK came in sixth place and the USA came in at the bottom of the table with a total of 1,660 attempted attacks per thousand computers. According to Jon Ramsey, CTO for SecureWorks, the reasons for the difference in number of attempted attacks per country could comprise many things. This range from the overall Internet speeds in a country and how proactive the ISPs are in protecting their clients to general user education on security. The ratio of Windows, Mac and Linux users in a country will also make a big difference.

Source: Help Net Security, July 5, 2010
<http://www.net-security.org/secworld.php?id=9525>

5.3 RISK OF CYBER THREATS SERIOUSLY UNDERESTIMATED

A new study by the Ponemon Institute demonstrates that a vast majority of enterprises of all sizes regularly fall victim to advanced cyber threats. At the same time, more than half of these organizations recognize their defensive technologies, personnel and budget as "inadequate". The group of nearly 600 IT and IT security leaders provided insight into a wide variety of issues and concerns surrounding business risk and the security of enterprise technology environments. "Information security is not a set-it-and-forget-it proposition," said Larry Ponemon, Chairman and Founder of the Ponemon Institute. "In our discussions with key stakeholders, it is obvious that while threats are evolving quickly, defenses continue to lag. More than 70% of organizations reported that advanced threats are evading traditional security stalwarts such as AV and IDS. With more than 83% believing that their organizations have been recently targeted by advanced threats (41% citing

they are frequent targets) the need for training security personnel and using new methods for attack detection and remediation is a growing requirement.

Source: Help Net Security, July 6, 2010
<http://www.net-security.org/secworld.php?id=9534>

5.4 HOUSE VOTES TO BLOCK NET PORN ON GOVERNMENT PCS

A recent vote in the U.S. House of Representatives seemed straightforward enough: government computers must block viewing or downloading porn. After all, a series of news reports have highlighted, in scandalous detail, how some financial regulators earning six-figure salaries were watching porn at work as Wall Street imploded. The measure, which arrived in the form of a 111-page amendment sponsored by House Appropriations Chairman David Obey, a Wisconsin Democrat, says on the second-to-last page: "None of the funds made available in this act may be used to maintain or establish a computer network unless such network blocks the viewing, downloading, and exchanging of pornography."

Source: CNET News, July 8, 2010
http://news.cnet.com/8301-13578_3-20010067-38.html

5.5 FACEBOOK TO PROMOTE NEW U.K. SAFETY APPLICATION

Though it has successfully resisted pressure to install a mandatory "panic button" on users' home pages, Facebook has permitted the U.K.'s Child Exploitation and Online Protection Centre (CEOP) to build an application for its platform that members of the social-networking site can use to report online abuse directly to CEOP or seek advice about potential dangers of the Web. Called ClickCEOP, the app has been released following negotiations and eventually a partnership with Facebook. On Tuesday, U.K.-based Facebook members

between the ages of 13 and 18 will see an ad on the site that encourages them to install it the same way that they would install any other third-party Facebook app. CEOP also has a new "fan page" with resources geared towards young Facebook users in the U.K. While Facebook had been resistant to CEOP's campaign, the company confirmed to CNET that it had never actually blocked or prohibited a third-party "panic button" application, a conclusion that could easily be jumped to. Also, the application was not officially launched by Facebook, but the social network will help spread the word about it.

Source: CNET News, July 12, 2010
http://news.cnet.com/8301-13577_3-20010244-36.html

- Pharmacy spam retained the top spot with 64 percent of all spam.

Source: Help Net Security, July 13, 2010
<http://www.net-security.org/secworld.php?id=9575>

5.6 CYBERCRIMINALS INCREASE EFFECTIVENESS WITH MULTI-STAGE ATTACKS

Cybercriminals have been increasing the effectiveness of their individual outreach by creating multi-stage, also known as blended, attacks, which combine messaging and Web elements. They use email or search engine results to lure victims to sites hosting spam advertising, malware, or phishing. A new Commtouch report analyzes the many methods fraudsters, malware distributors and spammers use to inspire their victims to action, such as leveraging trusted brands like Apple and Google; holidays, or current events, for example, the Football World Cup. Some highlights from the Commtouch report:

- Pornography remains the Web site category most infected with malware.
- India has surpassed Brazil for the title of the country with the most zombies (13 percent of the world's total).