



# Cyber Security Policy Research Division

## CYBER SECURITY INCIDENT OUTSIDE MALAYSIA

Report No. 10 – July 2010

16 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

<b>DISCLAIMER .....</b>	<b>iii</b>
<b>1 FRAUD .....</b>	<b>1</b>
<b>1.1 FAKE TOY STORY 3 SCAMS CREATES MALIGN BUZZ.....</b>	<b>1</b>
<b>1.2 "OMG MOTHER WENT TO JAIL" FACEBOOK SCAM SPREADS     VIRALLY.....</b>	<b>1</b>
<b>1.3 OMG! PROFILE SPY TARGETING FACEBOOK USERS .....</b>	<b>1</b>
<b>2 HACK THREAT/INTRUSION .....</b>	<b>2</b>
<b>2.1 FLAW COULD EXPOSE 'MILLIONS' OF HOME ROUTERS.....</b>	<b>2</b>
<b>2.2 AUSSIE HACKER PLEADS GUILTY TO BANKING TROJAN SCAM .....</b>	<b>2</b>
<b>3 PHISHING ATTACK .....</b>	<b>2</b>
<b>3.1 BANK OF AMERICA PHISHING SCAM.....</b>	<b>2</b>
<b>3.2 'FREEWARE' PHISHING KIT DUPES KIDDIES .....</b>	<b>2</b>
<b>3.3 WOW PLAYERS TARGETED WITH PHISHING EMAILS.....</b>	<b>3</b>
<b>4 SPAM .....</b>	<b>3</b>
<b>4.1 TOP 12 SPAM-RELAYING COUNTRIES .....</b>	<b>3</b>
<b>5 MALWARE.....</b>	<b>3</b>
<b>5.1 P2P INCREASINGLY FAVORED BY MALWARE ATTACKERS.....</b>	<b>3</b>
<b>5.2 MARIPOSA MALWARE AUTHOR ARRESTED IN SLOVENIA.....</b>	<b>4</b>
<b>5.3 GOOGLE HAS TWO TIMES MORE MALWARE THAN BING, YAHOO! AND     TWITTER COMBINED.....</b>	<b>4</b>
<b>6 OTHERS.....</b>	<b>5</b>
<b>6.1 SKIMMING DEVICES ON GAS PUMPS SENDING STOLEN CARD     NUMBERS VIA BLUETOOTH.....</b>	<b>5</b>
<b>6.2 LACK OF COMPUTER SECURITY EXPERTS WEIGHS HEAVY ON U.S.     CYBER DEFENSE .....</b>	<b>5</b>

**6.3 GET NOTIFIED OF SUSPICIOUS FACEBOOK ACCESS TO YOUR ACCOUNT ..... 5**

**6.4 REPORT: NSA, PENTAGON OFFICIALS LINKED TO CHILD PORN ..... 6**

**6.5 ATMS HACKED AND SPITTING UP MONEY AT BLACK HAT ..... 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 FAKE TOY STORY 3 SCAMS CREATES MALIGN BUZZ

Scammers have taken advantage of the buzz around the recent release of *Toy Story 3* to bait bogus survey sites and pop-up software scams. The bogus sites ostensibly punting complete, steaming media downloads of the latest adventures of Buzz and Woody actual redirect the credulous through a thicket of potentially harmful and time wasting material. As with a previous similar scam themed around the series finale of *Doctor Who*, the whole exercise is a con designed to trick gullible surfers into completing dodgy surveys while offering nothing in return, warns Chris Boyd, a security researcher at Sunbelt Software. Prospective marks are invited to turn off Ad-Block before completing the surveys, a tactic designed to enable the perpetrators of the scams to rake in extra income by serving pop-up ads.

**Source: The Register, July 20, 2010**  
[http://www.theregister.co.uk/2010/07/20/toy\\_story\\_3\\_scams/4](http://www.theregister.co.uk/2010/07/20/toy_story_3_scams/4)

### 1.2 "OMG MOTHER WENT TO JAIL" FACEBOOK SCAM SPREADS VIRALLY

Sophos is warning Facebook users about a new scam that is spreading quickly across the social network pretending to be a link to a photograph of a baby boy taken by his mother. The messages, which are being posted on users' Facebook pages, read "OMG!! Guys, you have to see this: This mother went to jail for taking this pic of her son!" Similar to the recent "Never Gonna Drink Coca-Cola Again" scam, the attack encourages users to "like" a Facebook page, tricking them into sharing the link on their wall before they are able to access the image. When users have completed these necessary steps, a fake security check then appears asking users to take part in an

online survey. The scammers make money from directing traffic to the online surveys, which gather personal information. In some cases the surveys claim that participants will be sent a free iPad as a prize for participating.

**Source: Help Net, July 21, 2010**  
<http://www.net-security.org/secworld.php?id=9618>

### 1.3 OMG! PROFILE SPY TARGETING FACEBOOK USERS

Facebook users are a curious lot, and one of the things that seemingly regularly pique their interest is the opportunity to see who views their profile. Posts that read "OMG OMG OMG... I can't believe this actually works! Now you really can see who views your profile!!! WOAHA --> (link to site)" popping up on users' pages and Friend Feeds have been seen in the last couple of days, but all Facebook warns, don't go falling for this recycled scam. The provided links will take you to pages outside Facebook designed to convince you that if you post the exact message you have fallen for on different places on your Facebook page, you will be allowed to download Profile Spy a fake application that supposedly lets you see who viewed your profile. Of course, after you have done all this, you won't be able to download the offered application, but you will be asked to complete a number of surveys and to register for a mobile service that costs \$19.99 per month.

**Source: Help Net Security, July 26, 2010**  
<http://www.net-security.org/secworld.php?id=9635>

## 2 HACK THREAT / INTRUSION

### 2.1 FLAW COULD EXPOSE 'MILLIONS' OF HOME ROUTERS

According to Craig Heffner, a researcher at security consultancy Seismic, millions of household routers are susceptible to a flaw that creates a handy means for hackers to hijack surfing sessions or hack into home networks. The DNS rebinding-related security flaw affects kit from Linksys Belkin and Dell, among others. DNS rebinding have been around for years. Heffner claims he has discovered a new variant of the theme, which initially involves luring a surfer into visiting a website containing malicious code. This code uses a "Jedi-mind trick" to circumvent the same-origin policy, thereby allowing JavaScript-based malware to penetrate private home networks supported by vulnerable hardware. The sleight of hand discovered by Heffner involves establishing an attack site which runs malicious script that means a visitor's own IP address is presented as one of the site's alternative IP addresses, thereby granting a trusted status to a malign site. Modern browsers are designed to block earlier types of such attacks but not with this particular scenario.

**Source: The Register, July 19, 2010**  
[http://www.theregister.co.uk/2010/07/19/home\\_router\\_hack/](http://www.theregister.co.uk/2010/07/19/home_router_hack/)

### 2.2 AUSSIE HACKER PLEADS GUILTY TO BANKING TROJAN SCAM

An Australian hacker has pleaded guilty to infecting 3,000 computers with an information-stealing Trojan. According to UPI reports, Anthony Scott Harrison, 21, from the Black Forest area near Adelaide, pleaded guilty on Monday to seven computer hacking offences over the attempted cybercrime scam. He used an unnamed strain of malware to swipe bank logins and credit card details. Harrison also

admitted creating a 74,000-strong bot army of compromised Windows machines capable of launching denial of service attacks.

**Source: The Register, July 27, 2010**  
[http://www.theregister.co.uk/2010/07/27/oz\\_vxer\\_guilty\\_plea/](http://www.theregister.co.uk/2010/07/27/oz_vxer_guilty_plea/)

## 3 PHISHING ATTACK

### 3.1 BANK OF AMERICA PHISHING SCAM

Phishing emails purportedly coming from Bank of America are nothing new. Every now and then scammers roll out a slight variation on the previous one, and the latest targeted to Bank of America customer to re-confirm their account information is no exception. ScanSafe reports that the link provided for signing in to online banking points to a [gramsbbq.org/bain](http://gramsbbq.org/bain) (a website belonging to barbecue establishment in California), which in turn automatically redirects the users to the phishing page which is hosted on [chasingarcadia.com](http://chasingarcadia.com) another legitimate, but compromised, site belonging to a Canadian band. The use of compromised sites for redirecting and hosting phishing pages is a technique successfully used by many scammers, since it allows the emails to bypass reputation filters and community-based trust reporting.

**Source: Help Net Security, July 16, 2010**  
<http://www.net-security.org/secworld.php?id=9592>

### 3.2 'FREWARE' PHISHING KIT DUPES KIDDIES

Skilled malware authors have duped less skilled cybercrooks into doing their dirty work with a new phishing kit. A "freeware" phishing kit posted onto hacker forums poses as a way to set up fraudulent websites pretending to be, for example, PayPal or webmail providers. Spam emails

masquerading as security checks are then distributed to hoodwink the credulous into handing over their login credentials. The proxy hackers will record some success, potentially stealing scores of credentials before their fake sites are taken offline. However, secret backdoor functionality in the Login Spoofer 2010 phishing kit means that the vast majority of stolen credentials are sent back to the original authors of the hacking tool, not the proxy hackers who use it. The approach allows the original authors of the phishing kit to harvest thousands of web and payment service credentials without monkeying around with spam campaigns by delegating the spade work to their unwitting minions. The "automated, cloud-based phishing kit" was developed in Algeria and features Arabic tutorials but runs in English, database security firm Imperva reports.

**Source: The Register, July 23, 2010**  
[http://www.theregister.co.uk/2010/07/23/freeware\\_phishing\\_kit\\_sheanigans/](http://www.theregister.co.uk/2010/07/23/freeware_phishing_kit_sheanigans/)

### **3.3 WOW PLAYERS TARGETED WITH PHISHING EMAILS**

According to F-Secure, World of Warcraft players are once again targeted by a phishing scheme. Emails purporting to come from Blizzard Entertainment the creators of WoW have hit inboxes around the world, claiming that the Blizzard is investigating recent thefts of accounts and requiring of the users to change/restore their passwords. Of course, the email contains a link that takes the user to a web page that does not belong to Blizzard. Apart from the suspicious link, a good indication that this email is not coming from Blizzard are the noticeable grammatical and language errors. F-Secure experts have investigated further and discovered that the sender used a SMTP relay attack to spoof the "From" address to make it look like the email is coming from Blizzard, but is in fact coming from an individual Hotmail email account.

**Source: Help Net Security, July 26, 2010**  
<http://www.net-security.org/secworld.php?id=9633>

## **4 SPAM**

### **4.1 TOP 12 SPAM-RELAYING COUNTRIES**

Sophos has published its latest report into the top twelve spam-relaying countries, covering the second quarter of 2010. The United States continues to be the number one spam polluter, piping out 15.2% of all global spam messages an increase from 13.1% in the first quarter of 2010. The UK a nation that last year fell out of the spam hall of shame also saw a significant rise in the proportion of spam it relayed. With a total output of 4.6% of the world's spam, this puts the UK in fourth place overall compared with ninth earlier this year.

1. United States 15.2%
2. India 7.7%
3. Brazil 5.5%
4. UK 4.6%
5. South Korea 4.2%
6. France 4.1%
7. Germany 4.0%
8. Italy 3.5%
9. Russia 2.8%
10. Vietnam 2.7%
11. Poland 2.5%
12. Romania 2.3%

**Source: Help Net Security, July 19, 2010**  
<http://www.net-security.org/secworld.php?id=9593>

## **5 MALWARE**

### **5.1 P2P INCREASINGLY FAVORED BY MALWARE ATTACKERS**

Cisco released its 2Q10 Global Threat Report, which is an aggregation of data and insights on threats from Cisco Security

Intelligence Operations. The report merges the most current threat analysis from Cisco IPS, Cisco IronPort, and Cisco ScanSafe data. Key highlights include:

- Eastern Europe encountered the highest rate of web-based malware in 2Q10, followed by South America and China
- Continuous high saturation in 2Q10, coupled with recent P2P malware developments, suggest that peer-to-peer file shares are becoming increasingly favored by users and malware attackers alike.
- 7.4 percent of all web-based malware encounters in 1Q10 resulted from search engine queries and nearly 90 percent of all Asprox encounters in June of 2010 were the results of links in search engine results pages
- Companies in the Pharmaceutical and Chemical vertical were the most at risk for web malware encounters, experiencing a heightened risk rating of 400 percent in 1Q10 and 543 percent in 2Q10

**Source: Help Net Security, July 27, 2010**  
<http://www.net-security.org/secworld.php?id=9641>

## 5.2 MARIPOSA MALWARE AUTHOR ARRESTED IN SLOVENIA

A 23-year old Slovenian hacker that goes by the handle "Iserdo" has been arrested for developing the code that allowed the three alleged Spanish Mariposa botnet herders to infect some 13 million personal, corporate, bank and government computers in more than 190 countries. The arrest is the result

of a massive investigation that included the FBI, Spanish authorities, the Slovenian Criminal police, and the Mariposa working group (comprising the Georgia Tech Information Security Center, Defence Intelligence, Panda Security, and other international security experts). Jeffrey Troy, the FBI's deputy assistant director for the cyber division, says that more arrests will likely follow those of other operators that bought the software package from the hacker. He considers Iserdo's arrest a major break in the investigation, since it will prevent further updating of the code and/or organizing another botnet that will take control of the still infected computers, i.e "orphaned" bots.

**Source: Help Net Security, July 19, 2010**  
<http://www.net-security.org/secworld.php?id=9648>

## 5.3 GOOGLE HAS TWO TIMES MORE MALWARE THAN BING, YAHOO! AND TWITTER COMBINED

Barracuda released its Barracuda Labs 2010 Midyear Security Report, revealing data from two key areas: search engine malware and Twitter use and crime rate. Barracuda Labs conducted a study across Bing, Google, Twitter and Yahoo!, over a roughly two-month period. The analysis reviews more than 25,000 trending topics and nearly 5.5 million search results. Key highlights from the search engine study include:

- Overall, Google takes the crown for malware distribution turning up more than twice the amount of malware as Bing, Twitter and Yahoo! combined when searches on popular trending topics were performed. Google presents at 69 percent; Yahoo! at 18 percent; Bing at 12 percent; and Twitter at one percent.

- Over half of the malware found was between the hours of 4:00 a.m. and 10:00 a.m. GMT.
- In general, activity is increasing on Twitter: more users are coming online; True Twitter Users are tweeting more often, and even casual users are becoming more active. As users become more active, the malicious activity also increases.

**Source: Help Net Security, July 29, 2010**  
<http://www.net-security.org/secworld.php?id=9654>

## 6 OTHERS

### 6.1 SKIMMING DEVICES ON GAS PUMPS SENDING STOLEN CARD NUMBERS VIA BLUETOOTH

A maintenance worker at a Shell gas station located in Florida was the first one to notice that a gas pump he was checking had been fitted with a credit card skimming device. After he reported the fact to the Alachua County Sheriff's Office, detectives have been sent out to check every pump on every gas station within a mile of the Interstate 75 and they found three skimming devices on gas pumps on three different gas stations. The U.S. Secret Service was notified and joined the investigation, which brought to light the fact that the devices use Bluetooth to transmit the stolen information to the thieves behind this scheme, and that these gas pumps are not the first ones that have been compromised. The Secret Service is aware of a larger crime wave involving this very tactic hitting the Southeast of the country, and they believe that all these instances could be tied to a single Miami gang.

**Source: Help Net Security, July 19, 2010**

<http://www.net-security.org/secworld.php?id=9602>

### 6.2 LACK OF COMPUTER SECURITY EXPERTS WEIGHS HEAVY ON U.S. CYBER DEFENSE

When it comes to defending itself from cyber attacks, the U.S. is one of the most vulnerable countries in the world, since many civilian and military operations are essentially dependent on data networking. We have recently seen what could happen if a foreign government or extremely organized group of knowledgeable individuals targets the U.S. infrastructure. According to NPR, while China has put training computer security experts at the top of their list of national priorities encouraging individuals to choose it for a career, organizing competitions to spot them, recruiting caught hackers and "reward" them with more training and a job for the government the U.S. have really dropped the ball on this issue. James Gosler, a veteran cyber security expert judges that at this time, there are around 1,000 people in the U.S. who are knowledgeable enough to perform the role of a national cyber defender, government agencies and big business need 20 or 30 times that number of experts. A recently published report by the Center for Strategic and International Studies confirms this opinion. They call it a "human capital crisis in cybersecurity".

**Source: Help Net Security, July 20, 2010**  
<http://www.net-security.org/secworld.php?id=9611>

### 6.3 GET NOTIFIED OF SUSPICIOUS FACEBOOK ACCESS TO YOUR ACCOUNT

For all of you who haven't figured it out already, there is a simple way to make sure that if someone breaks into your Facebook account and misuses it, you know it immediately. All that's needed is a simple

change to your settings that takes less than 5 seconds altogether. Just log in into your Facebook account, go to your Account Settings, change your Account Security, and choose to receive notifications for login from new devices. You will receive an email notification if someone accesses your account from a computer or mobile device you haven't used before almost instantly, and if you have activated Facebook Mobile, you can receive the notification by SMS.

**Source: Help Net Security, July 22, 2010**  
<http://www.net-security.org/secworld.php?id=9624>

#### **6.4 REPORT: NSA, PENTAGON OFFICIALS LINKED TO CHILD PORN**

According to a report in The Boston Globe, dozens of National Security Agency, DARPA, and other Pentagon officials purchased and downloaded child pornography over the Internet. The newspaper said it obtained more than 50 pages of documents revealing that the government workers identified in an internal probe included NSA contractors with top secret clearances, one of whom has fled the country and is believed to be hiding in Libya. Another involved a person working at the super secret National Reconnaissance Office, which operates the military's spy satellites, who was transferred to a field office and has not been charged with a crime. In the United States, it is legal to possess obscene materials, which are generally defined as hardcore pornography involving consenting adults. It is also legal to possess non-obscene pornography. But the knowing possession of child pornography is a federal felony. Some, but not all, of the Pentagon workers were charged as a result of the internal investigation, which had not previously been made public. In one 2007 case, the Globe said, a national security official possessed 8,400 pictures, and 200 movies "that were evidence of receipt of child pornography" and was sentenced to five years in prison.

**Source: CNET News, July 23, 2010**  
[http://news.cnet.com/8301-13578\\_3-20010067-38.html](http://news.cnet.com/8301-13578_3-20010067-38.html)

#### **6.5 ATMS HACKED AND SPITTING UP MONEY AT BLACK HAT**

Security researcher Barnaby Jack has managed to make two unpatched ATMs from two major vendors spit out cash during his demonstration at the Black Hat conference in Las Vegas. He accessed the ATM manufactured by Tranax Technologies with software that can remotely operate the machine, and then installed a rootkit that revealed administrative passwords and account PINs, which allowed him to wrest money from it. The ATM made by Triton Systems was compromised locally, by using a key that he acquired over the Internet and that enabled him to gain access to the internal components of the machine and to install a rootkit from a USB drive. He thinks the reason to this high incidence of vulnerable machines is due to the fact that ATMs haven't been targeted as much as, let's say, Microsoft products. If they had, the manufacturers would have had give much more attention to secure development. He also says that vulnerable ATMs are very easily located, since they return specific responses when contacted by phone or with queries to IP addresses.

**Source: Help Net Security, July 29, 2010**  
<http://www.net-security.org/secworld.php?id=9657>