

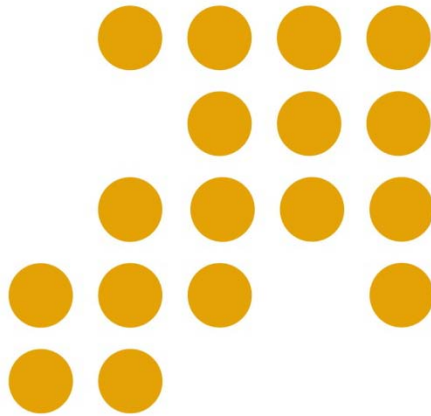


Cyber Security Policy Research Division

CYBER SECURITY INCIDENT OUTSIDE MALAYSIA

Report No. 5 – May 2010

01 May 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 LATEST SCAMS AND HOW TO AVOID THEM	1
1.2 FORGED CHECKS PASS FLAWED EXAMINATION PROCESS	1
1.3 CLUELESS FRAUDSTER TARGETS THINKGEEK	1
2 MALWARE	2
2.1 TWITTER-CONTROLLED BOTNET SDK AT LARGE	2
3 HACK THREAT/INTRUSION	2
3.1 EX-CON HELPS FEDS FOIL AN ATM HACKING SCHEME	2
3.2 WORDPRESS USERS UNDER ATTACK	2
3.3 ATTACK DETECTORS ON CPUS EXPOSES BACKDOORS	3
3.4 LATVIAN "ROBIN HOOD" HACKER'S IDENTITY REVEALED	3
4 SPAM	3
4.1 FAKE AMAZON "DEAL OF THE DAY" EMAILS DOING ROUNDS	3
4.2 CANADIAN PHARMACY NO LONGER TOP SPAMMED BRAND	3
4.3 SMALL ISP WINS IN COURT, SPAMMERS MUST PAY	3
5 PHISHING ATTACK	4
5.1 ANTI-PHISHING PHYLLIS TRAINING GAME	4
5.2 ONE CRIME SYNDICATE RESPONSIBLE FOR MOST PHISHING ATTACKS	4
5.3 FACEBOOKDIGITS PHISHING SCAM	4
6 OTHERS.....	4
6.1 DETECT AND MITIGATE DNS SECURITY THREATS WITH ACTIVETRUST DNS	4
6.2 LESSONS TO BE LEARNED FROM FACEBOOK PRIVACY CHANGES ...	5

6.3 MONEY MULES WANTED 5
**6.4 FACEBOOK SOCIAL PLUG-INS PRIVACY CONCERNS SORTED OUT BY
PALO ALTO NETWORKS 5**
6.5 HOW SECURE IS OUR PERSONAL HEALTHCARE INFORMATION?..... 5
6.6 U.S. FEDERAL DATA SECURITY VULNERABILITIES..... 6
**6.7 NETWORK ADMINS WORRY ABOUT EMPLOYEE USE OF SOCIAL
MEDIA 6**
**6.8 FACEBOOK’S CHANGES CLASH WITH EUROPEANS’ EXPECTATIONS
OF PRIVACY 6**
6.9 LAPTOP THEFT EXPOSES DATA ON 201,000 ARMY RESERVISTS 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 LATEST SCAMS AND HOW TO AVOID THEM

Over the years, we have come to rely on the Internet to fulfill many of our needs - the need to keep in touch with our friends and colleagues, the need to save time and our nerves when doing shopping, executing financial transactions, submitting our tax returns, and many other things we did before in person or by phone. But, on the Internet is way easier to impersonate someone and to scam people. You can never be completely certain that the person you're "talking" to is the person you think it is. Malicious links that lead to malware, phishing schemes and spam seem to be everywhere you look. We have all been on the receiving end of emails that purport to be from our bank, various organizations and institutions, online retailers, "friends" in need of money, "girls" who want to chat with us, the IRS, and many other legitimate-seeming sources. In time, we have grown accustomed to receiving at least a couple of them a day and to spot the bad apples. Or so we think. The truth is that as long as these scams work, they will be present. And since they are still here, it means that people still fall for them. Although, one must admit that the scammers are becoming more ingenious by the day. Jean Chatzky, the financial editor for NBC's "Today", explains the latest scams and how to avoid them.

Source: Help Net Security, May 03, 2010
<http://www.net-security.org/secworld.php?id=9231>

1.2 FORGED CHECKS PASS FLAWED EXAMINATION PROCESS

The recent cases of two Texan women who had their personal information and checking

account numbers stolen and used to validate bogus checks, have brought into the spotlight a questionable check processing methodology used by some retailers and banks. According to CBS11TV, the method practically allows identity thieves to shot down any possibility of investigation because of a lack of actual evidence, and makes the retailers and the financial institutions unwitting accomplices in the crime. Linda Jacobs and Angie Carden are the aforementioned identity theft victims whose names found their way on hot checks used by the criminals to buy things at Kroger and Wal-Mart stores. Finding out that they were suspected of fraud was shocking, but luckily for them they managed to prove that they had nothing to do with it (Carden was even in the hospital at the time when the checks were written). Even though instances of successful check forgery are getting rarer as the years pass, there are always loopholes in the checking process that can be taken advantage of. In these two cases, the flaw in the system consists of retailers treating checks as electronic debits. When a customer hands one over to the cashier, the check is given back to the customer after the information has been copied, and sometimes the retailers don't even perform a visual scan.

Source: Help Net Security, May 03, 2010
<http://www.net-security.org/secworld.php?id=9230>

1.3 CLUELESS FRAUDSTER TARGETS THINKGEEK

Popular online retailer, ThinkGeek, is - like many other retailers - sometimes targeted by fraudsters. To diagnose potential fraudulent orders, they usually double-check orders that sport a billing address in one country, and a shipping address in another. One of the latest attempts was rather poorly executed, but must have made customer service personnel laugh. When asked for a photo ID, the customer - one "James Neff" - has sent in a photoshopped

version of a photo that can be found on the Internet and is of a sample passport that famous comedian and television host Stephen Colbert received from the Hungarian Ambassador to the U.S when he appeared on his show. In the original picture, the name on the passport is Colbert's, but "James Neff" photoshopped (badly) his name over it. ThinkGeek's customer service spotted the fraud.

Source: Help Net Security, May 07, 2010
<http://www.net-security.org/secworld.php?id=9260>

2 MALWARE

2.1 TWITTER-CONTROLLED BOTNET SDK AT LARGE

Huge armies of zombified computers unanimously executing the commands sent by their master – that's what comes in the mind of a computer user at the sound of the word "botnet". Fortunately enough, writing a bot is an extremely tedious task that takes a lot of in-depth programming knowledge, so not everyone can become a botmaster overnight, despite the obvious financial advantages. BitDefender has released an emergency update to protect against a potential pandemic caused by the emergence of a botnet self-development kit controllable via the popular social media service Twitter. In order to create their custom bot, an attacker only has to launch the SDK, enter a Twitter username that would act as a command & control center and modify the resulting bot's name and icon to suit their distribution method.

Source: Help Net Security, May 14, 2010
<http://www.net-security.org/secworld.php?id=9295>

3 HACK THREAT / INTRUSION

3.1 EX-CON HELPS FEDS FOIL AN ATM HACKING SCHEME

Thor Alexander Morris had a plan. The plan involved reprogramming certain ATMs so that they would overpay him when he made a withdrawal, giving out \$20 instead of \$1 bills - or, at least, this is what the prosecutors say. He allegedly asked Brian Rhett Martin, an ex-con from Texas, to help him identify the locations in and around Houston where specific ATM models are located - ATMs that have a flawed feature that allows a specific pass code to be used to gain administrative access and reprogram the machine.

Source: Help Net Security, May 05, 2010
<http://www.net-security.org/secworld.php?id=9246>

3.2 WORDPRESS USERS UNDER ATTACK

WordPress-based websites have once again become the target of attacks. This time around, the hacked websites are hosted by various ISPs: DreamHost, GoDaddy, Media Temple and Bluehost, and there are also rumors floating around that other PHP-based platforms could also have been affected. The H Security reports that it is still unknown which security hole has been exploited to launch the attack, which infects the websites with malicious scripts that allow fake AV to be installed on the systems of people who visit the sites in question. To avoid detection, the malware prevents some browsers (Firefox and Google Chrome) from alerting potential visitors about the malicious nature of the website.

Source: Help Net Security, May 12, 2010
<http://www.net-security.org/secworld.php?id=9284>

3.3 ATTACK DETECTORS ON CPUS EXPOSES BACKDOORS

How can you be sure that the CPU on your computer hasn't been tampered with and is not stealthily collecting your data for someone else to use? Adam Waksman and Simha Sethumadhavan, two scientists from Columbia University, have presented TrustNet and DataWatch - lightweight attack detectors that are incorporated into the microprocessor and issue alerts when it executes an unexpected amount of instructions or shows signs of being modified for malicious purposes. "Our mechanisms leverage the fact that multiple components within a microprocessor must necessarily coordinate and communicate to execute even simple instructions, and that any attack on a microprocessor must cause erroneous communications between micro architectural subcomponents used to build a processor," say the two scientists in their paper.

Source: Help Net Security, May 13, 2010
<http://www.net-security.org/secworld.php?id=9291>

3.4 LATVIAN "ROBIN HOOD" HACKER'S IDENTITY REVEALED

The identity of the Latvian hacker who, earlier this year, hacked and publicly disclosed tax office data showing that state officials were still getting a enormous salaries in spite of the official government policy of cutting corners, has been revealed by the Latvian police. Hiding under the handle "Neo" is Ilmars Poikans, a researcher from the University of Latvia's Computer Science department, reports The Baltic Course. He was taken into custody on Tuesday, interrogated and a criminal process has been launched against him, but has since been released pending arraignment or trial.

Source: Help Net Security, May 14, 2010

<http://www.net-security.org/secworld.php?id=9292>

4 SPAM

4.1 FAKE AMAZON "DEAL OF THE DAY" EMAILS DOING ROUNDS

Fake Amazon newsletters have lately become regular visitors in inboxes around the world, says Trend Micro. With "Amazon.com Deal of the Day" in the subject line, coming from seemingly legitimate Amazon email addresses, and looking a lot like legitimate newsletters with product endorsements coming from the online retail giant, the spam campaign was probably pretty successful. A click on any image or link embedded into the email would lead the victim to a possibly malicious site.

Source: Help Net Security, May 03, 2010
<http://www.net-security.org/secworld.php?id=9227>

4.2 CANADIAN PHARMACY NO LONGER TOP SPAMMED BRAND

According to the statistics by M86 Security Labs, Canadian Pharmacy - the long-standing champion of spammed affiliate brands - made way for the new reigning king: Canadian RX Drugs. Following the two pharma leaders is the usual assortment of Rolex watches, designer handbags, slimming pills and gambling-related spam.

Source: Help Net Security, May 06, 2010
<http://www.net-security.org/secworld.php?id=9255>

4.3 SMALL ISP WINS IN COURT, SPAMMERS MUST PAY

Asis Internet Service, a smallish Californian ISP that counts only 4 employees, has 2.6 millions reasons to celebrate. The ISP filed

a lawsuit against a company named "Find a Quote" and its CEO, for sending them 25,000 spam emails over a 18-month period. The judge ruled in favor of the plaintiff and awarded almost \$2.6m in damages, although it's doubtful they will ever see the money placed on their account.

Source: Help Net Security, May 07, 2010
<http://www.net-security.org/secworld.php?id=9261>

5 PHISHING ATTACK

5.1 ANTI-PHISHING PHYLLIS TRAINING GAME

Wombat Security Technologies announced the release of Anti-Phishing Phyllis, a training game to teach employees and customers how to spot fraudulent emails. In this training game, users help a fun fish character named Phyllis teach her school of fish how to avoid phishing traps in fraudulent emails. Traps covered in the game include fake links, malicious attachments, cash prizes, "respond-to" emails asking for sensitive information and much more.

Source: Help Net Security, May 11, 2010
<http://www.net-security.org/secworld.php?id=9277>

5.2 ONE CRIME SYNDICATE RESPONSIBLE FOR MOST PHISHING ATTACKS

A single electronic crime syndicate employing advanced malware was responsible for two-thirds of all the phishing attacks detected in the second half of 2009 - and was responsible for the overall increase in phishing attacks recorded across the Internet, according to a report released today by the Anti-Phishing Working Group (APWG). The report authors found that the Avalanche phishing

gang was responsible for some 66 percent of all phishing attacks launched in 2H2009. Avalanche successfully targeted some 40 banks and online service providers, and vulnerable or non-responsive domain name registrars and registries. "Avalanche" is the name given to the world's most prolific phishing gang, and to the infrastructure it uses to host phishing sites. This criminal enterprise perfected a system for deploying mass-produced phishing sites, and for distributing malware that gives the gang additional capabilities for theft.

Source: Help Net Security, May 12, 2010
<http://www.net-security.org/secworld.php?id=9283>

5.3 FACEBOOKDIGITS PHISHING SCAM

Facebook users have lately been targeted by a clever phishing scam. The phishing website, whose looks evoke those of the social network, is trying to convince potential victims that they can now take advantage of a service that will allow them to get a "Facebook phone number".

Source: Help Net Security, May 12, 2010
<http://www.net-security.org/secworld.php?id=9285>

6 OTHERS

6.1 DETECT AND MITIGATE DNS SECURITY THREATS WITH ACTIVETRUST DNS

Internet Identity (IID) released ActiveTrust DNS, designed to detect, diagnose and mitigate DNS security threats. By hijacking DNS translations, attackers can drive unsuspecting surfers and corporate users to malicious sites, making large parts of the 'Net largely useless or insecure'. They can also intercept corporate e-mail, financial transactions, and other highly sensitive data and personal information. Recent DNS

hijackings of CheckFree, Comcast, Baidu and Twitter highlight how vulnerable organizations are to DNS exploits.

Source: Help Net Security, May 04, 2010
<http://www.net-security.org/secworld.php?id=9239>

6.2 LESSONS TO BE LEARNED FROM FACEBOOK PRIVACY CHANGES

The recent Facebook privacy changes, the public outcry they caused and the petition by a group of U.S. senators to the Federal Trade Commission to restrict the amount of personal information that online social networks can use, have brought into the spotlight the question of just how much the revealed information can hurt you. Highly personal information such as a full birth date can help cyber thieves, and your street address, phone number and a status that says that you're on vacation can be used by burglars. Revealing your children's names and photos can help child predators. Social networks can expose the users to abuse - whether from harassment, scams, identity theft or malware infection. These are all things that we are aware of deep down inside, but often choose not to think about because of the 'it-won't-happen-to-me' conviction.

Source: Help Net Security, May 05, 2010
<http://www.net-security.org/secworld.php?id=9245>

6.3 MONEY MULES WANTED

Reading about people unwittingly becoming money mules for cyber criminals, a lot of people wonder if they would be able to spot if the offer they received or searched for is illegitimate. F-Secure shows us an example (or three) of a mule recruiting campaign - a website purporting to be the official page of Finha Capital, a Finnish company offering financial services.

Source: Help Net Security, May 05, 2010

<http://www.net-security.org/secworld.php?id=9242>

6.4 FACEBOOK SOCIAL PLUG-INS PRIVACY CONCERNS SORTED OUT BY PALO ALTO NETWORKS

Facebook users in enterprises are susceptible to having their confidential data shared with third parties because of recent changes at Facebook, which cause behavioral data from its users to be made available unless a user explicitly opts out. Palo Alto Networks released new functionality that enables enterprises to control Facebook Social Plug-ins, empowering users to continue to embrace Facebook while mitigating any privacy concerns. The new default Facebook privacy settings are designed to share private and corporate information with advertisers and other third parties. In enterprises, this policy has major implications, as there is no central way for IT security teams to protect their users from the unknown and – in almost all cases – unwanted privacy impact, which involves the sharing of behavioral and website information with Facebook and its advertising customers. Palo Alto Networks combines three identification technologies to provide visibility and control over Facebook-related functionality, users and content.

Source: Help Net Security, May 06, 2010
<http://www.net-security.org/secworld.php?id=9249>

6.5 HOW SECURE IS OUR PERSONAL HEALTHCARE INFORMATION?

Forty-seven percent of IT security professionals believe their personal healthcare information is less secure than it was 12 months ago according to a survey by nCircle. The online survey of 257 security professionals was conducted

between February 4 and March 12, 2010, and covered a range of security topics including smartphones, healthcare, cloud computing and social media. “The Patient Protection and Affordable Care Act is expected to intensify the already huge push for electronic health records, and many IT professionals and consumers feel their personal health information is less secure than ever,” says Alex Quilter, healthcare security strategist with nCircle. “The healthcare industry’s focus on patient care is imperative, but should not come at the expense of patient privacy.”

Source: Help Net Security, May 10, 2010
<http://www.net-security.org/secworld.php?id=9268>

6.6 U.S. FEDERAL DATA SECURITY VULNERABILITIES

Data security vulnerabilities that exist within the U.S. Federal agencies are due to employees’ use of unsecure methods to exchange information, such as FTP – despite the Secure File Sharing Act, which the U.S. House of Representatives passed on March 24, 2010 to prevent government employees from using peer-to-peer file-sharing software, including FTP. This is one of the results of a survey by MeriTalk and Axway. According to the Federal File Transfer Report, Federal employees are exposing data to cyber criminals. Though 71 percent of Federal IT and information security professionals are concerned with Federal file transfer security, 54 percent admit they do not currently monitor for FTP use within their agencies.

Source: Help Net Security, May 10, 2010
<http://www.net-security.org/secworld.php?id=9269>

6.7 NETWORK ADMINS WORRY ABOUT EMPLOYEE USE OF SOCIAL MEDIA

According to findings a survey of 353 network administrators by Amplitude

Research, four-in-ten (40%) were either "extremely concerned" (18%) or "moderately concerned" (22%) with employee use of social media being a security threat to their company. Only 12% were "not at all concerned," while 22% were "slightly concerned" and 26% "somewhat concerned." When asked in an open-ended manner, "What concerns you most about employee use of social media at your company?", network administrators mentioned viruses (22%), unproductive / time wasted (21%), security / intrusion risk (19%), data / information leaks (16%), privacy issues (7%), malware (5%), and bandwidth usage (4%). This year's survey found that nearly four-in-ten (39%) of the network administrators were "kept up at night" worrying about a security breach to their network in 2010, which was significantly higher than in 2009 (27%).

Source: Help Net Security, May 12, 2010
<http://www.net-security.org/secworld.php?id=9280>

6.8 FACEBOOK’S CHANGES CLASH WITH EUROPEANS’ EXPECTATIONS OF PRIVACY

Europeans are well-known for their high privacy expectations and demands. Another proof of that is a letter that the Article 29 Working Party (an independent European Commission advisory body) has sent to Facebook, in which they say it is "unacceptable that the company fundamentally changed the default settings on its social-networking platform to the detriment of a user." This is, of course, not the first negative reaction Facebook has to face for their newly made changes to its Privacy settings. In the US, the Electronic Privacy Information Center and the Federal Trade Commission made their disapproval known. Canada and some European countries have also previously called into question some of Facebook's data policies.

Source: Help Net Security, May 13, 2010

<http://www.net-security.org/secworld.php?id=9288>

6.9 LAPTOP THEFT EXPOSES DATA ON 201,000 ARMY RESERVISTS

Personal data on 207,000 U.S. army reservists has recently been stolen along with three laptops from the offices of a government contractor (Serco Inc.). The U.S. Army Reserve Command has begun notifying the reservists of this security fail via letters that offer apologies and assurances that "something" will be done to prevent these things from happening again: "At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data," it says in the letter. According to Brian Krebs, the data in question was held on a CD-Rom that was in one of the laptops at the time the theft occurred, and encompasses names, addresses and Social Security numbers of the reservists. It is also likely it contained some data that belongs to spouses and dependents of the reservists.

Source: Help Net Security, May 13, 2010
<http://www.net-security.org/secworld.php?id=9289>