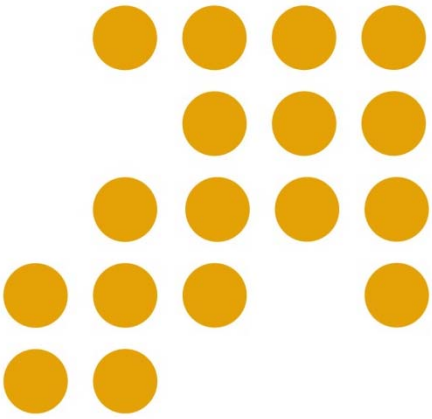
Cyber Security Policy Research Division

CYBER SECURITY INCIDENT OUTSIDE MALAYSIA

Report No. 11 – August 2010

1 August 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

1 FRAUD

1.1 POLICE NAB SIX IN UK ONLINE BANKING FRAUD STING

According to Metropolitan Police in London, six people have been arrested for allegedly running a phishing operation that netted at least £358,000 (US$569,000) and compromised more than 20,000 bank accounts and credit cards. Five men and one woman between the ages of 25 and 40 were arrested on suspicion of conspiracy to commit online banking fraud and violations of the Computer Misuse Act. The gang allegedly sent out spam to lure people to fake web sites purporting to be major banks that asked for passwords and other information. The fraudsters then transferred money out of their bank account or abused their credit cards. Police said the credit card-related fraud could be as high as £3 million ($4.7 million). The bank account fraud could be as much as £1.14 million ($1.8 million), although police said they haven't established how much the group may have profited.

Source: Computerworld, 4 August 2010
http://www.computerworld.com/s/article/9180140/Police_nab_six_in_UK_online_banking_fraud_sting

1.2 FIREFOX 4 BETA CRACK SPREADS TROJAN TO TOTAL IDIOTS

Scammers are trying to con gullible marks into getting infected via a fake Firefox 4.0 beta download scam. Preview editions of the next version of Firefox are available for download directly from Mozilla at no charge. So it's pretty obvious that offers of Firefox 4 beta cracks or a keygen are entirely bogus and almost certainly malicious. Fraudsters are therefore hoping the hoodwink the truly clueless into running a supposed Firefox 4 keygen tool or crack, both of which are being promoted via scam-boosting Twitter accounts. Surfers who follow through with the scam are also directed towards a site hosting a smorgasbord of other digital parasites.

Source: The Register, 6 August 2010
http://www.theregister.co.uk/2010/08/06/firefox_crack_scam/

1.3 CORRUPT REPAIR ENGINEER JAILED FOR BANK FRAUD ATTEMPT

A corrupt laptop repair engineer has gone to jail for nine months after he was convicted of hacking into the laptop of one of his customers. Grzegorz Zachodni, 30, was caught browsing through pictures in a private folder and attempting to hack into an online banking account during a *Sky News* investigation into computer repair services. As part of the investigation a laptop with a simple fault, rigged to ensure that its webcam covertly filmed "repairs", was deposited at Laptop Revival in Hammersmith. Zachodni used his access to the machine to browse photos of the reporter in a bikini in a folder marked private and to attempt to access Facebook, eBay and online banking accounts using a "password file" left on the machine. A total of six attempts were made to access the online banking account.

Source: The Register, 9 August 2010
http://www.theregister.co.uk/2010/08/09/corrupt_comp_repair_tech_jailed/

1.4 DOMAIN NAME REGISTRATION SCAM HALTED

The Federal Trade Commission has permanently halted the operations of Canadian con artists who allegedly posed as domain name registrars and convinced thousands of U.S. consumers, small businesses and non-profit organizations to pay bogus bills by leading them to believe they would lose their web site addresses unless they paid. Settlement and default judgment orders signed by the court will bar

the deceptive practices in the future. In June 2008, the FTC charged Toronto-based Internet Listing Service with sending fake invoices to small businesses and others, listing the existing domain name of the consumer's web site or a slight variation on the domain name, such as substituting ".org" for ".com." The invoices appeared to come from the businesses' existing domain name registrar and instructed them to pay for an annual "WEBSITE ADDRESS LISTING." The invoices also claimed to include a search engine optimization service. Most consumers who received the "invoices" were led to believe that they had to pay them to maintain their registrations of domain names. Other consumers were induced to pay based on Internet Listing Service's claims that its "Search Optimization" service would "direct mass traffic" to their sites and that their "proven search engine listing service" would result in "a substantial increase in traffic." The FTC's complaint charged that most consumers who paid the defendants' invoices did not receive any domain name registration services and that the "search optimization" service did not result in increased traffic to the consumers' Web sites.

Source: Help Net Security, 10 August 2010
http://www.net-security.org/secworld.php?id=9716

1.5 CLICK FRAUD BOTNET UNPICKED

Cybercrooks use of botnets to make money by sending spam or launching denial of service attacks has become a well-understood business model. But the controllers of networks of compromised PCs have other ways of turning an illicit profit, including using rogue traffic brokers to defraud reputable brands. Trend Micro has been on the trail of one particular gang of click fraud crooks for over 18 months. The gang is originally from Estonia, although there are loose connections with the UK, which hosts a shell company for a click broker selling web traffic that plays an important role in the complex scam. David Sancho, a security researcher at Trend Micro's Labs, explained that the scam uses short-lived bots to redirect web traffic from compromised machines. Surfers seeking to visit Yahoo, for example, might be redirected via a third-party service before arriving at their destination, earning an unscrupulous broker a few cents in the process.

Source: The Register, 11 August 2010
http://www.theregister.co.uk/2010/08/11/click_fraud_botnet/

1.6 HIPPO-VOMITING ANACONDA SCAM TARGETS FACEBOOK USERS

Sophos is warning Facebook users about a virally spreading survey scam. The attack involves a rogue application that automatically posts status updates and wall posts on affected user profiles with the following message, "OMG, this is the biggest and scariest snake I have ever seen, check out this video." The link takes users to a rogue Facebook application which tricks them into granting permission for the app to access their profile, list of friends and to be allowed to re-post the offending message as a status update and wall post. "Each time a victim completes a survey, the scammers make some commission. Even if you don't take the survey, the rogue application has already abused your Facebook account, changing your status message and spreading an advert for the alleged 'shocking video' to your news feed, spreading the scam even further," said Graham Cluley, senior technology consultant at Sophos.

Source: Help Net Security, 11 August 2010
http://www.net-security.org/secworld.php?id=9717

2 HACK THREAT / INTRUSION

2.1 HACKING INTO GSM FOR ONLY $1500

A researcher at the DefCon hackers' has demonstrated kit for spoofing GSM base stations, allowing even those on a limited budget to intercept phone calls and text messages. The audiences attending the talk by Chris Paget were able to see their own handsets transferring to his spoofed base station, with calls receiving a recorded message explaining that the security had been compromised. The basis of the attack isn't new: the attacker sets up a base station advertised as belonging to a compatible network operator and handsets locally switch to the stronger signal. In a live attack the base station then connects to the real cellar network and passes authentication tokens back and forth as though it wasn't there. GSM communications are supposed to be encrypted between the genuine network at the handset, but in some countries strong encryption isn't allowed so the network informs the handset not to encrypt the communications. The handset is supposed to pop up a warning when this happens, but doesn't, so rogue base stations can ask the handset not to encrypt anything and then listen in.

Source: The Register, 2 August 2010
http://www.theregister.co.uk/2010/08/02/gsm_cracking/

2.2 HACKER USES GOOGLE STREET VIEW DATA TO STALK ITS VICTIMS

A security researcher has devised an attack suitable for stalking and similarly creepy endeavors that uses JavaScript and geo location data from Google to pinpoint a victim's precise location. In a talk titled “How I Met Your Girlfriend,” at the Black Hat conference, hacker Samy Kamkar demoed the technique, which he cleverly dubbed an XXXSS. Here's how it works:

- Kamkar lures the victim to a website that uses JavaScript to extract her router's Media Access Control address and report the unique identifier to the hacker. If JavaScript is unpalatable for some reason, there are other ways to do this.
- Kamkar plugs the pilfered MAC address into Google Location Services. Within seconds, he has a map showing the victim's location within a few hundred feet.

Over the past few years, Kamkar has used XSS, or cross-site scripting, exploits to achieve a variety of hacks. As the author of the Samy Worm, he served a brief stint in jail for unleashing a self-replicating exploit in 2005 that added more than 1 million friends to his MySpace account and in the process knocked the site out of commission. More recently, he's used XSS to burrow into firewalls and home routers.

Source: The Register, 3 August 2010
http://www.theregister.co.uk/2010/08/03/google_street_view_hack/

2.3 FORMER SAN FRANSISCO NETWORK ADMIN TERRY CHILDS SENTENCED TO PRISON

After a drawn out trial that saw City of San Francisco administrator Terry Childs being convicted of violating California state hacking laws by deliberately locking the authorities out of the city's FiberWAN network by refusing to disclose administrative passwords, he has finally been sentenced to four years in prison. According to Computerworld, during the trial the prosecution characterized Childs as a "power hungry control freak that couldn't be managed." Childs himself maintained that he was only doing his job and that his

immediate supervisor was not qualified to be given the passwords. After 12 days of refusing to surrender them, he eventually surrendered the passwords to Gavin Newsom, the mayor of the city.

Source: Help Net Security, 9 August 2010
http://www.net-security.org/secworld.php?id=9701

3 PHISHING ATTACK

3.1 PHISHERS TARGET MOBILE PHONE USERS

According to Symantec reports, mobile phone users in the UK and Norway have been targeted by malicious emails purporting to come from their mobile service providers, claiming that the users have to confirm their billing information. The emails contain a link to a legitimate but compromised web page that masquerades as the page for the billing and payment services of the provider. If the victim fails to notice the unusual URL of the page, he/she will be giving over to the phishers a great amount of personal and financial information that can be effectively used to steal their identity and their money. After the victims have entered and confirmed the information, the page redirects them to the legitimate site of the provider, thus making the illusion complete.

Source: Help Net Security, 5 August 2010
http://www.net-security.org/secworld.php?id=9691

3.2 PHISHERS OFFER FALSE SECURITY IN EXCHANGE FOR YOUR FACEBOOK PASSWORD

It is possible that the recent launch of Facebook's Safety page gave phishers the idea of launching one of their own, since Symantec recently detected a phishing website posing as a "Security and Privacy Update" page. But, while the legitimate one offers to keep you abreast of security issues plaguing the social network, the fake one tries to convince you that you only have to enter your email and password in order to be protected from spam, hackers and others "who want to ruin your facebook". Setting aside the fact that the phishing page is full of spelling errors, awkward sentences, and simply looks fake even at first glance, you will notice that the page is not hosted on Facebook and tries to masquerade itself as a website related to a security update.

Source: Help Net Security, 10 August 2010
http://www.net-security.org/secworld.php?id=9715

4 SPAM

4.1 FACEBOOK BUG COULD GIVE SPAMMERS NAMES, PHOTOS

Facebook is scrambling to fix a bug in its website that could be misused by spammers to harvest user names and photographs. It turns out that if someone enters the e-mail address of a Facebook user along with the wrong password, Facebook returns a special "Please re-enter your password" page, which includes the Facebook photo and full name of the person associated with the address. The feature helps people understand if they've mistyped their e-mail address at login, but it could be misused by spammers to get information on Facebook's 500 million users. A spammer with an e-mail list could write a script that enters the e-mail addresses into Facebook and then logs the real names. This could help make a phishing attack more realistic. Scammers have taken a special interest in Facebook over the past few years, and criminals such as the people who wrote the Koobface worm may well take an interest in the bug, said Roger Thompson, chief research officer with antivirus vendor AVG.

Source: Computerworld, 11 August 2010

http://www.computerworld.com/s/article/9180592/Facebook_bug_could_give_spammers_names_photos

4.2 JUNK MAIL KINGPIN HELD ON CHILD ABUSE CHARGES

Notorious spammer Leo Kuvayev is being held on remand in his native Russia over child sex charges. Kuvayev, 38, who occupies the second spot on Spamhaus' ROKSO list of the world's worst spammers, is accused of molesting 50 children from Moscow orphanages. The suspect has been held on remand since last December but news of his detention only broke this week via a report by ex-*Washington Post* reporter Brian Krebs. Kuvayev was indicted last August and arrested in September following a police investigation prompted by complaints by one of the girls he allegedly abused. Kuvayev, who specialises in pharmacy and pirated software spam and holds dual Russian and American citizenship, was successfully sued for violations of the CAN-SPAM Act back in 2005. Spamhaus cites Kuvayev as a pioneer in the use of image-based spam as a means of sidestepping spam filters and the use of botnet networks of compromised PCs to distribute junk mail.

Source: The Register, 12 August 2010
http://www.theregister.co.uk/2010/08/12/spammer_held_on_child_abuse_charges/

5 MALWARE

5.1 POISONED ANGELINA FLICK HITS TORRENTS

Cybercrooks have begun using booby-trapped QuickTime files to infect internet pirates' computers. Malicious files posing as the recent Angelina Jolie film *Salt* are now available on file sharing networks. When users attempt to view these poisoned downloads a prompt is generated offering to download "update codecs" which actually fake files loaded with Trojan horse malware. At first the attack was thought to rely on an unpatched flaw in QuickTime, but Apple told Trend Micro this is not the case, and the attack relies solely on social engineering trickery.

Source: The Register, 2 August 2010
http://www.theregister.co.uk/2010/08/02/quicktime_trojan_assault/

5.2 HOAX FACEBOOK VIRUS MAKES MORE TROUBLE THAN A REAL VIRUS

A hoax Facebook virus is spreading rapidly across the social network. Many users have been hoodwinked into forwarding an inaccurate warning about the spread of non-existent malware that claims a girl committed suicide over a post her father wrote on her Facebook wall. No such tragedy has occurred but many are forwarding the wrong-headed message creating confusion in the process. According to net security firm Sophos, people are passing on the warning in the mistaken belief they are helping Facebook friends to avoid a threat. In reality, they are spreading a hoax about a non-existent virus infection. The bogus warning is arguably causing more of a nuisance than a genuine malware infection.

Source: The Register, 6 August 2010
http://www.theregister.co.uk/2010/08/06/facebook_virus_hoax/

5.3 MALWARE GANG STEAL OVER £700K FROM ONE BRITISH BANK

According to security researchers, a banking Trojan attack has led to the fraudulent withdrawal of more than $1m from online banking accounts maintained with a UK bank since the start of July. Web-based malware based on the infamous Zeus cybercrime toolkit is being used to

steal money via the unnamed online banking system. Researchers at the M86's Security Labs came across the attack after discovering the botnet's command & control centre, which is hosted in Moldova. Victims were infected by a Zeus banking Trojan variant while browsing the net. The Trojan swiped the customer's online banking ID and hijacked their online banking sessions, reportedly only targeting victims who had substantial balances. Most such attacks include the use of phishing middlemen to obtain funds from compromised accounts and transfer them by untraceable wire transfer to the Eastern European masterminds behind the scam.

Source: The Register, 10 August 2010
http://www.theregister.co.uk/2010/08/10/zeus_uk_bank_ripoff/

5.4 FIRST SMS-SENDING ANDROID TROJAN REPORTED

Security experts warned on Tuesday about what is believed to be the first Trojan targeting Android-based mobile devices that racks up charges by sending text messages to premium-rate numbers. According to Denis Maslennikov, senior malware researcher at Kaspersky Lab, the Trojan-SMS malware, dubbed "Trojan-SMS.AndroidOS.FakePlayer.a," is being distributed via an unknown malicious web site. Users are prompted to install a "media player application" that is a little bigger than 13 kilobytes, but which is hiding the Trojan inside. Like all Android apps, the program asks for permission to do certain things upon install. In this case it asks for permission to send SMS messages, with a prompt that identifies it as a "service that costs you money," as well as to read or delete data and collect data about the phone and the phone ID, Kaspersky and Lookout said. Once installed, the Trojan starts sending messages behind the scenes that cost several dollars per message, without the device owner knowing it. To tell if you are affected, review your bills for any premium messages. Lookout also suggests that if you have recently downloaded a media player, check the permission to make sure the app is not sending SMS.

Source: CNET News, 10 August 2010
http://news.cnet.com/8301-27080_3-20013222-245.html

6 OTHERS

6.1 SAUDI ARABIA POSTPONES BLACKBERRY BAN

Last week, the United Arab Emirates and Saudi Arabia announced their plans for an imminent blockade of some BlackBerry functions if BlackBerry manufacturer Research in Motion doesn't make it possible for the government to keep encrypted communication under surveillance. RIM responded by saying that third-party access to its servers (where the encrypted data is sent) was impossible, but they are currently in negotiations with both governments on whether something can be done to satisfy both parties and allow the countries' BlackBerry users to use their devices as they were meant to be used. Reuters reports that the planned Saudi Arabia shutdown of Blackberry's Messenger that was meant to be executed on Friday has been postponed until midnight today, because RIM and Saudi's three mobile carriers are working on setting up three servers that will send encrypted data through Saudi Arabia before sending it to the servers in Canada and the U.K.

Source: Help Net Security, 9 August 2010
http://www.net-security.org/secworld.php?id=9708

6.2 COLLEGES BREACH STUDENTS' SENSITIVE INFORMATION

College students nationwide can be especially vulnerable to identity theft because they often give out personally identifiable information. Some universities have even been known to use a student's Social Security Number (SSN) as their student identification number, sometimes displayed on a student ID card. Over the last year, Privacy Rights Clearinghouse (PRC) estimates that more than one million students, alumni and faculty have been affected by a data loss, or breach, of personal information. Since July 2009, an estimated 72 breaches in 30 states have been reported, according to PRC. PRC shows that in approximately 88 percent of these instances, a student or individual's SSN was exposed. Personal information can be breached in various ways, including hackers gaining unlawful access to computer files containing student information (even SSNs), or a dishonest or disgruntled university employee obtaining computer files containing sensitive records and then selling the records to savvy identity thieves.

Source: Help Net Security, 9 August 2010
http://www.net-security.org/secworld.php?id=9704

6.3 RUSSIAN CHARGED WITH SELLING CREDIT CARD NUMBERS ONLINE

A Russian man accused of selling stolen credit card numbers online for nearly a decade has been arrested in Nice, France, and faces charges in an indictment unsealed Wednesday. Vladislav Anatolievich Horohorin, 27, was arrested by French authorities on Saturday as he attempted to board a flight to Moscow. Horohorin, who called himself BadB online, advertised himself as one of the largest sellers of stolen credit and debit cards worldwide. Horohorin advertised the availability of stolen credit card information through web forums, and directed purchasers to create accounts at dumps.name, a fully automated dumps vending website operated by Horohorin and hosted outside the U.S. The website was designed to assist in the exchange of funds for the stolen credit card information. Horohorin allegedly directed buyers to fund their dumps.name accounts through services including web money, an online currency service hosted in Russia.

Source: Computerworld, 11 August 2010
http://www.computerworld.com/s/article/9180589/Russian_charged_with_selling_credit_card_numbers_online