CyberSecurity MALAYSIA

Cyber Security Policy Research Division

CYBER SECURITY INCIDENT OUTSIDE MALAYSIA

Report No. 7 – June 2010

01 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

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 THREE INDICTED IN $100 MILLION SCAREWARE FRAUD SCHEME

An international cybercrime scheme caused Internet users in more than 60 countries to purchase more than one million bogus software products, causing victims to lose more than $100 million. The charges allege that the defendants, through fake advertisements placed on various legitimate companies' websites, deceived Internet users into falsely believing that their computers were infected with malware or had other critical errors to induce them to purchase scareware software products that had limited or no ability to remedy the purported but nonexistent, defects. The alleged scheme is widely regarded as one of the fastest-growing and most prevalent types of Internet fraud.

Source: Help Net Security, June 01, 2010
http://www.net-security.org/secworld.php?id=9355

1.2 "HIDDEN IRON MAN 2 SCENE" FACEBOOK SCAM

Curiosity - that drives to know new things - is a double-edged sword. It fuels our inclination towards exploration and, consequently, learning, but it can also occasionally lead us to trouble. When it comes to clicking on malicious links that pop up on messages on social networking sites, it seems that our curiosity works heavily against us. The latest example of this natural human tendency getting exploited is the "hidden Iron Man 2 scene" scam lurking on Facebook. The link in the message redirects users to a website outside Facebook, where they are told to click on the provided "Like" button in order to view the video. Luckily for all of them, the link does not lead to malware or a malicious website that could compromise their system. But, instead of seeing the video, the victims are presented with an unexpected request of confirming their Facebook account. Offering them $110 in phone credit, the scammers' trick the gullible users into sharing their mobile number - making them part of their pool of numbers that will be receiving unsolicited offers via text messages.

Source: Help Net Security, June 08, 2010
http://www.net-security.org/secworld.php?id=9379

2 MALWARE

2.1 FREE APPS INSTALL SPYWARE ON MACS

Intego, a security company said, Mac users downloading free screensavers and a video converter app from several popular download sites will also get spyware that installs a back door, collects data, and sends encrypted information to remote servers. According to a list compiled by Intego, the high-risk spyware, dubbed OSX/OpinionSpy, was being installed along with nearly 30 screensavers developed by a company called 7art and an app called MishInc FLV to MP3. The spyware, a Windows version of which has existed since 2008, is not contained in the apps but is downloaded during the installation process. It is often marked as a "market research" program called PremierOpinion that claims to collect browsing and purchasing information for use in market reports, but it can also come with no warning or message. In some cases the infected computer will not work correctly and the user will need to force a reboot. In addition, deleting the original app or screensaver will not delete or interfere with the spyware. In some cases the infected computer will not work correctly and the user will need to force a reboot.

Source: CNET News, June 01, 2010
http://news.cnet.com/8301-27080_3-20006502-245.html

2.2 MALWARE FOUND LURKING IN APPS FOR WINDOWS MOBILE

Scammers are distributing apps for Windows Mobile-based smartphones that have malware hidden inside that makes calls to premium-rate numbers across the globe, racking up expensive bills to the phone's owner. According to John Hering, chief executive and founder of mobile security provider, the apps--3D Anti-Terrorist game, PDA Poker Art, and Codec pack for Windows Mobile 1.0--are being distributed on as many as nine popular download Web sites, including DoDownload, GearDownload, and Software112. Once the app is installed the virus wakes up and starts dialing premium-rate numbers like in Somalia and the South Pole. He added that victims may not know about the problem until they get their phone bill and see that it's $50 or $100 higher than it should be. "Users need to be aware of what they are downloading and make sure it is a reputable source and from a reputable developer," he said.

Source: CNET News, June 04, 2010
http://news.cnet.com/8301-27080_3-20006882-245.html

2.3 TWO MEXICAN BOTNETS TAKEN DOWN

A week ago, Trend Micro was alerted to a phishing attack that was aimed at Spanish-speaking users and was discovered to be originating from a Mexican botnet. The attack was using the news of a missing girl and her violent death to try to get the visitors to download a video. Of course, the video in question was no such thing, but a client program of bot. Searching deeper, Trend Micro researchers managed to access the botnet's C&C center, and discover - and publish - details about its management functions and interface, as well as get a good look into what this botnet was able to do. They found out that it was also responsible for downloading malware (Zbot information stealers and fake AVs) on the target computers, and for targeting users with phishing attacks that impersonated PayPal's site and that of the largest bank in Mexico. Finally, they named it Tequila botnet. Since then, the Tequila botnet has been taken down - surprisingly enough, by its owners. The researchers speculate that the reason behind this decision was the fact that they have exposed the proxy servers and hosts.

Source: Help Net Security, June 10, 2010
http://www.net-security.org/secworld.php?id=9397

3 HACK THREAT / INTRUSION

3.1 IT PROS ARE HACKING THEIR OWN ENTERPRISES TO KEEP INTRUDERS OUT

A survey of IT security professionals has discovered that 83% consider commercial applications, the ones you buy off the shelf, to be riddled with code flaws and vulnerabilities. Fortify Software found that 56% believe these flaws could allow hackers to exploit these software vulnerabilities. As a result, security professionals are making heavy investments in penetration and code testing, combined with application scanning, to try and build security into the software. Half of the IT security professionals also admitted to hacking, with 73% of these respondents doing so to test the strength of their own network's defenses, 13% for fun or out of curiosity, and 3% targeting their efforts at the competition. Of those in this survey that admitted to previous hacking knowledge and experience, 42% learnt in their twenties and 14% in their teens. Most people learnt to hack at work -- 29%; on the Internet, 26%; at University, 13%; and 8% gained their hacking skills whilst still at school and 8% used friends to help them hone their talent.

Source: Help Net Security, June 02, 2010

http://www.net-security.org/secworld.php?id=9358

3.2 REMOTE WORKING POSES THREAT TO CORPORATE SECURITY

A recent survey of 200 UK IT directors has found that 92 percent believe that, by allowing more staff to work remotely, they are increasing their security risks. Even though all respondents said that their workforce was increasingly mobile, 80 percent admitted they found it difficult to manage and secure ever-more sophisticated mobile devices. Roger Hockaday from Aruba Networks comments, "As smart phones and other mobile devices become increasingly popular, they pose an increasing security threat to the unprepared business. For an easier life, many IT departments would choose to limit the devices that are allowed to access corporate networks – but with demand for the coolest gadgets often coming from senior executives – this choice is often taken away from them."

Source: Help Net Security, June 15, 2010
http://www.net-security.org/secworld.php?id=9413

4 PHISHING ATTACK

4.1 FACEBOOK ATTACK TRICKS USERS INTO 'LIKING' MALICIOUS LINKS

According to security firm Sophos, another clickjacking scam has hit Facebook, tricking hundreds of thousands of users to post messages to their pages saying that they like the malicious link. Like most of these scams, this one relies on social engineering and piques the interest of prospective victims with messages like:

- "LOL this girl gets OWNED after a POLICE OFFICER reads her STATUS MESSAGE."

- "This man takes a picture of himself EVERYDAY for 8 YEARS!!"

- "This Girl Has An Interesting Way Of Eating A Banana, Check It Out!"

Clicking on the links takes the visitor to what appears to be a blank page with just the message "Click here to continue." However, hidden in the page is code called an iFrame. When a visitor clicks anywhere on the page the iFrame publishes the message to the visitor's Facebook page. According to BitDefender's Malware City blog, Facebook has been notified and the malicious pages have been suspended.

Source: CNET News, June 01, 2010
http://news.cnet.com/8301-27080_3-20006478-245.html

4.2 IPAD PHISHING SCHEME ADVERTISED ON FACEBOOK

How would you like to get one of the much-anticipated iPad gizmos in exchange of simply filling up a mere survey? Well, the offer sounds pretty good – in fact, it sounds too good to be true and that’s what it is. The scheme is massively advertised on a Facebook Events page where about 2500 people signed up for the event and – probably – fell victim to the phishing attack. Concealed by a short URL, the target phishing page initially asks for some reasonable info such as the first name and the email address, and culminates with requiring a full set of details, including the full name, home address and phone numbers. In order to make the whole deal look legit, the attackers have thrown in logos belonging to high-profile media outlets, although the mentioned institutions have no clue about this initiative.

Source: Help Net Security, June 02, 2010
http://www.net-security.org/secworld.php?id=9369

4.3 FACEBOOK "101 HOTTEST WOMEN" CLICKJACKING ATTACK

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". Another clickjacking attack taking advantage of the "Like" button option has targeted Facebook users. The lure is very simple - follow the link to see the 101 hottest women in the world. According to Sophos, a click on the link takes you to a webpage with an image of Jessica Alba and a "Click here to continue…" link. Whether you follow it or click anywhere else on the page, your Facebook page will show you "liking" the page and probably lure your friends to click on it. This is the latest in the series of clickjacking attacks that has targeted Facebook users recently. The attackers take advantage of the users' curiosity by luring them with funny pictures and videos, and obtain their goal: the visitors create revenue for the owner(s) of the site, since it is part of an advertising network.

Source: Help Net Security, June 14, 2010
http://www.net-security.org/secworld.php?id=9409

5 OTHERS

5.1 CRITICAL IPHONE SECURITY ISSUE LEAVES YOUR CONTENTS EXPOSED

Most iPhone users are confident that using a passcode to secure their devices means that even if they lost them or they get stolen, their data will be protected from prying eyes. Unfortunately for them, Bernd Marienfeld, an information security professional, has discovered last week that the passcode protection can be bypassed by simply connecting the iPhone 3GS in question to a computer running Ubuntu 10.04. The iPhone can be tricked into allowing access to photos, videos, music, voice recordings, Google safe browsing database, game contents, and more, by switching it off and connecting it to the computer, then switching the iPhone back. Apple has been notified of the flaw, and they managed to reproduce it, but have yet to push out a fix or to say when it will be made available.

Source: Help Net Security, June 01, 2010
http://www.net-security.org/secworld.php?id=9352

5.2 ALL-INCLUSIVE SECURITY SOLUTION FROM RADWARE

Radware announced APSolute Attack Prevention, a security solution that connects several defenses together, allowing them to work synchronously and provide protection from hybrid network attacks that pose threats such as: application vulnerability, information theft, authentication defeat, malware spread, network anomalies, and more. Recent attacks in 2009 and 2010 such as the July 2009 cyber attacks and conficker malware show that attackers are using hybrid attack techniques that utilize multiple attack types and vectors. Today, organizations are deploying individual protection tools such as Intrusion Prevention System (IPS), Network Behavioral Analysis (NBA) and Denial of Service (DoS) protection. But, the use of multiple individual tools, increase costs and complexity while leaving networks and services unprotected against hybrid attacks. Designed for ecommerce, service providers and large enterprises, APSolute Attack Prevention is an all-inclusive attack mitigation solution, integrating different tools/modules, plus management and reporting, which need to work in a synchronized manner to detect and prevent hybrid threats.

Source: Help Net Security, June 01, 2010

http://www.net-security.org/secworld.php?id=9349

5.3 THE RISKS WHEN NETWORKS COLLIDE

The increasing convergence of multiple networks for voice, data, video and other services onto a single infrastructure based on IP, has the potential to leave serious gaps in security. Driven by the promise of reduced costs and increased flexibility, network convergence can expose organizations to unknown or unmitigated threats from malicious or malfunctioning infrastructure, devices and services. In addition, these problems are compounded if migration is not properly planned, structured and documented.

Source: Help Net Security, June 02, 2010
http://www.net-security.org/secworld.php?id=9356

5.4 TOP 5 FIFA WORLD CUP ONLINE RISKS-OTHERS

Lavasoft warned computer users to be aware of stealthy online traps set by cybercriminals to leverage public interest surrounding the 2010 FIFA World Cup – and issued advice to follow to make sure people enjoy the month-long tournament without becoming the target or victim of an attack. Events that draw such pervasive and ongoing public interest will, without a doubt, be used to propagate socially-engineered crimes - where users are manipulated into performing certain actions or disclosing confidential information.

Source: Help Net Security, June 02, 2010
http://www.net-security.org/secworld.php?id=9368

5.5 114,000 IPAD OWNERS' EMAILS AND ACCOUNT IDS EXPOSED

News that vulnerabilities on the AT&T network allowed a group calling itself Goatse Security to harvest emails and AT&T authentication IDs of 114,000 early-adopters of Apple's iPad shocked potential victims. Goatse Security has a history of warning about security vulnerabilities, and they managed to get their hands on the data by using a script on the AT&T's website. When provided with an ICC-ID as part of an HTTP request, the script would return the associated email address, in what was apparently intended to be an AJAX-style response within a Web application. The security researchers were able to guess a large swath of ICC IDs by looking at known iPad 3G ICC IDs, some of which are shown in pictures posted by gadget enthusiasts to Flickr and other internet sites, and which can also be obtained through friendly associates who own iPads and are willing to share their information, available within the iPad "Settings" application. But, what really made this news reverberate throughout the world is the fact that among the massive number of compromised accounts and email addresses, were those of many a military official, top politician, CEO and media mogul. Consequences of this breach may range from those email accounts being inundated with spam to device spoofing on the network or even traffic interception using the compromised authentication ID - the jury is still out on all the possible ramifications.

Source: Help Net Security, June 10, 2010
http://www.net-security.org/secworld.php?id=9392

5.6 DEGAUSS YOUR PHOTOCOPIER HARD DRIVES AND PREVENT DATA THEFT

The vulnerability of information stored on a computer hard drive has been recognized as a security risk for some time, but did you know that digital photocopiers and high-end laser printers also include a hard drive which can store and log all of your activity? Today’s copiers and printers harvest images of every scanned, faxed and printed document. Think for a moment about the vast quantities of information that you routinely print and copy: personnel files, financial reports, legal documents and commercial contracts – even your own passport. Now imagine this sensitive information falling into the hands of an unscrupulous third party. Some copiers now include built-in systems which encrypt copied files so that they cannot be recovered. However this solution is by no means fool-proof as someone with the right forensic software may still be able to recover fragments of data. The only way to safeguard complete and permanent erasure is to use a degausser.

Source: Help Net Security, June 15, 2010
http://www.net-security.org/secworld.php?id=9410