Cyber Security Policy Research Division

CYBER SECURITY INCIDENT OUTSIDE MALAYSIA

Report No. 6 – May 2010

16 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

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 RSA FIGHTS MAN-IN-THE BROWSER ATTACKS

RSA Man-in-the-Browser Solutions is a portfolio of anti-fraud services designed to provide defense against theft of online information. It includes newly enhanced transaction monitoring as well as risk-based authentication; Trojan detection and attack shut down; and intelligence to identify malware-infected enterprise environments. MITB attacks are designed by fraudsters to infect a web browser with malware that can result in modified web pages and transactions that are largely transparent to both the user and the host application.

Source: Help Net Security, May 19, 2010
http://www.net-security.org/secworld.php?id=9307

2 MALWARE

2.1 COMBAT THE MALVERTISING THREAT

Malicious advertising, also referred to as "malvertising," is a relatively new attack vector for cyber criminals that are quickly on the rise. With malvertising, fake malicious ads are delivered (often via advertising networks) to well-known websites as a way to reach millions of users at once on websites they normally trust. Unlike typical spam or virus attacks, which rely on victims to click on a link in an email or accidentally download an infected program, malvertising attacks are presented on popular websites and can download malicious code directly onto a user's computer when the victim views the compromised ad. By infiltrating an entire ad network, the criminal gains access to a broad number of syndicated websites that can spread malicious code even further. Millions of users have been infected by malvertising threats recently, as evidenced by the high-profile attacks on The New York Times, Gizmodo, TechCrunch, WhitePages.com and other sites. Based on data generated from Dasient's telemetry system, there are approximately 1.3 million malicious ads viewed per day.

Source: Help Net Security, May 18, 2010
http://www.net-security.org/secworld.php?id=9305

2.2 CRITICAL FACEBOOK BUG EXPOSES SENSITIVE INFORMATION

Yet another Facebook privacy bug has been discovered - this time by M.J. Keith, a senior security analyst with AlertLogic. The bug in question makes it possible for an attacker to access the account of a user and modify its content - if the user is duped into clicking on a link that leads to malicious Web site containing the Javascript code that exploits the cross-site request forgery flaw. According to the security advisory released on Wednesday by AlertLogic, the bug was spotted last week, and Facebook has been notified of it immediately. Three days later the social network confirms it has fixed it, but additional testing executed yesterday by Keith show that the bug is still present.

Source: Help Net Security, May 19, 2010
http://www.net-security.org/secworld.php?id=9312

2.3 NEW CLOUD POWERED ZONEALARM FREE FIREWALL

The new ZoneAlarm Free Firewall is powered by the community for stronger security - its DefenseNet service analyzes malware which was automatically reported by the community of millions of ZoneAlarm users. Once the safety or non-safety of a given program is determined, the information is then shared through the cloud, immediately blocking attacks and virtually eliminating the need for program alerts and interruptions. The software uses both signatures and heuristics to block dangerous Websites that standard browser security misses. ZoneAlarm also includes an Identity Checkup with IDENTITY GUARD that allows customers to see if their identity and personal information has been exposed, and then can protect that personal information with ongoing monitoring, alerts and more.

Source: Help Net Security, May 24, 2010
http://www.net-security.org/secworld.php?id=9327

3 PHISHING ATTACK

3.1 PHISHING PAGE STEALS PREPAID DEBIT CARD ACCOUNT INFORMATION

Many people don't have a regular or a big enough income to receive a debit card, but would still like to have one since it can be really handy when settling bills or shopping online. The answer to this problem? Prepaid debit cards. The good thing about this option is that if your card information is stolen and misused by cyber criminals, the monetary loss is limited to the (usually) small amount of money you have on your account. Since these cards are regularly used by low - to mid-income citizens, who really can't afford to lose even that amount, Symantec's revelation that there are phishing sites out there that are posing as the main website of a well known prepaid debit card service that will provide an almost lifesaving warning. The phishing site notifies the users that their account has been limited, and requires for them to enter the following confidential information in order to re-activate the account.

Source: Help Net Security, May 18, 2010
http://www.net-security.org/secworld.php?id=9306

3.2 VERY INTERESTING NEW TYPE OF A PHISHING ATTACK USING TABS

Aza Raskin from the Mozilla Firefox team found a pretty interesting new type of phishing attack that uses automatic change of *favicon* icon to make one of your tabs look like another web site.

Source: Help Net Security, May 25, 2010
http://www.net-security.org/secworld.php?id=9329

4 DOS

4.1 THE TELEPHONY DENIAL OF SERVICE ATTACK

While you're wondering why your phone is ringing incessantly and every time you answer it you hear nothing, a recorded message or an advertisement, thieves are likely pillaging your bank, online trading, and other money management accounts. The telephony denial of service (TDOS) attack is a way to divert your attention from what's really going on, and a way to make you unavailable to banks and other financial institutions. According to NJToday, the scheme works like this: cyber thieves have somehow managed to obtain your account information. They get in touch with the institution where you account is open, change information such as phone number and email address - or even bank account numbers, then keep your phone line busy and prevent the institution from checking up with you and verifying the changes and confirm transactions. When they do manage to get in touch with you, it is probably too late - your account has been emptied.

Source: Help Net Security, May 17, 2010
http://www.net-security.org/secworld.php?id=9301

4.2 PRISON SENTENCES IN THE SCIENTOLOGY CYBER ATTACK CASE

Brian Thomas Mettenbrink from Nebraska has been sentenced to a year in federal prison for his participation in the cyber attacks on the Church of Scientology's servers a couple of years ago. Metterbrink pleaded guilty in January. Back then, he admitted that he downloaded computer software from an “Anonymous” message board and used that software to bombard Scientology websites to the point that it impaired the integrity and availability of those websites in a variation of a DDoS attack.

Source: Help Net Security, May 25, 2010
http://www.net-security.org/secworld.php?id=9333

5 OTHERS

5.1 WEB BROWSERS LEAVE 'FINGERPRINTS' AS YOU SURF

An overwhelming majority of web browsers have unique signatures - creating identifiable "fingerprints" that could be used to track you as you surf the Internet, according to research by the Electronic Frontier Foundation (EFF). The findings were the result of an experiment EFF conducted with volunteers who visited a website that anonymously logged the configuration and version information from each participant's operating system, browser, and browser plug-ins - information that websites routinely access each time you visit - and compared that information to a database of configurations collected from almost a million other visitors. EFF found that 84% of the configuration combinations were unique and identifiable, creating unique and identifiable browser "fingerprints." Browsers with Adobe Flash or Java plug-ins installed were 94% unique and track able.

Source: Help Net Security, May 18, 2010
http://www.net-security.org/secworld.php?id=9303

5.2 60% OF FACEBOOK USERS CONSIDER LEAVING OVER PRIVACY

Will changes to Facebook's privacy settings be enough to address user concerns? A poll of 1588 Facebook users conducted by Sophos has revealed the extent of member concerns over the popular social network's privacy settings. The online survey shows that almost two thirds of Facebook users are considering leaving, with 16% of those polled claiming to have already stopped using Facebook as a result of inadequate control over their data. The poll asked Facebook users: Do you think you will quit Facebook over privacy concerns?:

Possibly: 484 - 30%
Highly likely: 469 - 30%
Already have: 254 - 16%
No: 191 - 12%
Don't think likely: 190 - 12%

Facebook has faced growing criticism over changes to the way that the social network can share user data across its site and with other websites. Concerns have centered on the complexity and 'opt-out' approach to sharing member information with wider networks.

Source: Help Net Security, May 19, 2010

http://www.net-security.org/secworld.php?id=9311

5.3 SOCIAL NETWORKING SITES PASSING ON USER DATA TO AD AGENCIES

Several social networking sites - including Facebook and MySpace - have apparently been sending users' data to advertising agencies - in spite of all the assurances and promises that this information is not shared with anyone without having previously asked the users for consent and receiving a thumbs-up. The Wall Street Journal maintains that it has discovered the concealed practice of the social networks of sending users' ID numbers and/or names to the agencies every time the users click on the ads, but that Facebook and MySpace have reacted expeditiously to the questions about it and have already changed much of the code that allowed this practice. The problem with the advertising agencies being given this information is that they could use it to mine other personal data from the profiles of those users, if they shared it with the network and if the privacy settings are set to minimum. The advertising agencies in question - including Yahoo's Right Media and Google's DoubleClick - claim that they haven't used the data because they didn't know the data was being sent in the first place.

Source: Help Net Security, May 21, 2010
http://www.net-security.org/secworld.php?id=9321

5.4 FACEBOOK USERS AGAINST DEFAULT SHARING OF THEIR PRIVATE DATA

A poll of 605 Facebook users conducted by IT security and data protection firm Sophos in the wake of the latest changes to the social network's privacy settings has revealed the vast majority of users would favour default settings that do not automatically share their information. Facebook this week simplified its privacy settings - allowing users to control who can see their friends and pages, but the network's attitude to data privacy continues to attract criticism as it makes changes to the level of control afforded to regular users.

Source: Help Net Security, May 27, 2010
http://www.net-security.org/secworld.php?id=9341