2011 International Conference on Computer Communication and Management
Proc .of CSIT vol.5 (2011) © (2011) IACSIT Press, Singapore

Collaborative Internet Threat Detection on Internet Infrastructure in Malaysia

Fajri Achmad Maulana[1+], Sahidan Abdulmana[1], Fauzan Alfariti[1] and Rahmat Abu Nong[2]

[1]International Islamic University Malaysia (IIUM)

[2]Malaysian Communication and Multimedia Commission (MCMC)

Abstract – Using a computer has its advantages as well as disadvantages. The number of people that use the Internet in Malaysia has increase gradually. At the same time, the numbers of threats that have been detected by various organizations are also increasing. Moreover, many systems in Malaysia are already computerized, in other word is controlled by the computer. As a result, it is making cyber space or internet not save and the cyber threats become as one of the serious threat for many organizations included Malaysia Government. Moreover, Malaysia Government has done a few things to overcome this kind of problem, such as made National Cyber Security Policy and also put the Internet Service Providers as one of the critical infrastructures in Malaysia. In this study, we propose a collaborative system model between Malaysian Communication and Multimedia Commission as a regulator, Malaysia Computer Emergency Response Team (MYCERT) as an agency and an Antivirus company as a private company. The collaboration system that we tried to propose, it will make SNSC (SKNMM Network Security Center) become more powerful and efficient in terms of internet threat detection. Our objective is to strengthen the internet threat detection system and to prevent the high impact of cyber threats that can happen on internet network in Malaysia. However, challenges that we might face when we want to implement this collaborative system model is always there.

Keywords: Network Security, Internet Threats Detection, Computer Security, Collaborative Internet Threats System**.**

1. Introduction

Nowadays, most of the people in the world use the Internet every time and everywhere with many purposes and access it from any device. The development of technologies make a lot of things possible happens in the clouds. Recently, the threat in the Internet was increased rapidly over the world and without known who are the attacker or who are the creator of the threats. According to the Sophos, in 2010, the number of spams reached 138 billion per day in the world and spam is just one of the threats existed. This number can increase again as well as other forms of threats. Many countries and organizations have monitored the trend of cyber threats that happen in cyber, and they have done many things like cyber campaign, cyber safe, and so on. Moreover, the Government of United States have shown its concern about the cyber threat when President Obama (2009) said in one of his speeches, "America's economic prosperity in the 21st century will depend on cyber security and this is also a matter of public safety and national security". It shows that the importance of securing the cyberspace on the internet. It is why we need to have taking serious action about it.

In Malaysia, there are steps taken to secure the internet such as help center, cyber security awareness program and so on. Many agencies and organizations like Malaysian Communication and Multimedia Commission (MCMC) in this country have done their work to secure the cyber space in Malaysia. MCMC has a lab called SKMM Network Security Center (SNSC) which to monitor internet traffic and to detect the threat from the internet traffic in and out of Malaysia. However, their work is still not finished due to the quick proliferation of new cyber threats. Malaysia Computer Emergency Response Team (MYCERT) showed in their 2010 statistics that the number of spam emailed was 155809, and the team has also alert that the number of web defacement incidents has increased [2].

Furthermore, there is still a lack of research done on collaborative effort among government organizations or the agencies with private organizations or companies to prevent Internet threats. In fact, some countries prefer buying the system (for monitor and detect Internet threats) from other countries rather than building the system on their own. In this paper, we will explore the development of threats in the Internet and identify the organizations that are responsible for controlling and monitoring the Internet in Malaysia. Our focus is on the threats that can overload the Internet traffic and the threats that have a big impact on the Internet environment in Malaysia. The paper it will also illustrate the concept of collaboration work between those agencies. This paper begins with the background of the issue of the Internet threat, next literature review, then the recommendation to overcome or mitigate the problems and the challenges.

2. Background

In 2008, out of 25,274,133 people in Malaysia, 15,868,000 people were using the Internet actively. This means that 62.8 % of all citizens in Malaysia were using the Internet in 2008. [3] Moreover, the penetration rate of telecommunications in Malaysia in first quarter also significant, 34.2% per 100 households have broadband, 43.6 % per 100 households have fixed line telephone, and about over 100% people per 100 populations use cellular phones [4]. In addition, they use the internet very actively from their home, office, schools, libraries, public places and even public transport.

In Malaysia, Malaysian Communications and Multimedia Commission initiated a security monitoring center called SNSC. The objective of SNSC is reducing the probability of cyber security risk by disseminating early warnings and share information among the stakeholders, thus minimizing any adverse impact to the overall Malaysian communication and multimedia industry [4]. This objective is equivalent to the National Cyber Security Policy (NCSP) and the 10th National Policy objective of the Communication and Multimedia Act 1998 [4]. Moreover, SNSC connected to the network security operation of the Internet Service Providers for the purpose of identified cyber-attacks and to raise early warning against cyber-attacks. SNSC also aware of public reports indicating web threats and mass defacement attack towards Malaysian websites [3].

We can see from two figures below that the top ten threats have detected by SNSC was dynamic. Figure 1 shows the top ten threats detected in the first quarter of 2010. It also shows that the threat on SMB services was the top list in the first quarter. However, in figure 2, it shows the threat on SMB services was no longer top of the list, whereas the threats on internet explorer DTHML edit Active control XSS become the top list in the second quarter. Furthermore, the other threats were not on the list of the top ten threats in the first quarter suddenly become top ten threats in quarter 2. In addition, figure 2 shows some threats were detected in two different signatures, for example, there is a threat on MS WIND Server at the same port but different vulnerabilities.

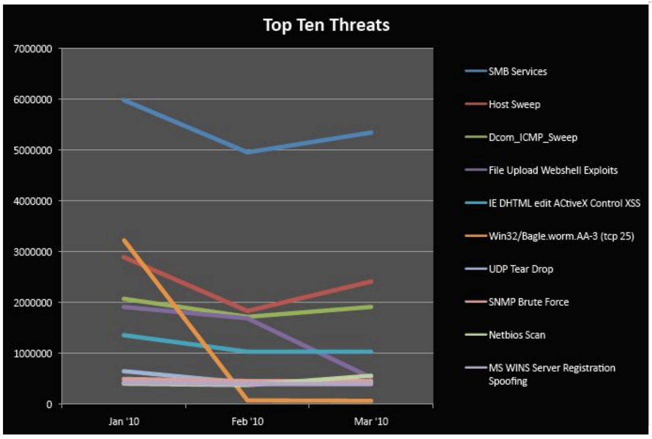

Figure 1.Top ten threats detected Q1 2010 in Malaysia by MCMC [19]

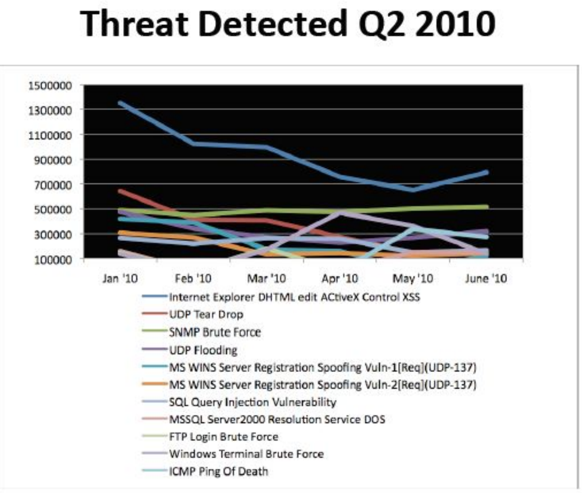

Figure 2.Top ten threats detected Q2 2010 in Malaysia by MCMC [4]

The signature of the Internet threat is very complex; when some of the threats are detected by some network Security Company, the attacker then tries to find a way to make a new threat or an evolution that can be undetected by a threat detection system. It is the reason why the database of the threat signature should be been update regularly, because the evolution of the Internet threat is very fast till the network security agency or company could not reach it.

3. Literature review

There is a case of the Internet threat monitoring in Japan that discussed in the paper. The paper describes algorithms for detecting which address spaces an Internet threat monitor listens to and presents empirical evidences that they are successful in locating the sensor positions of monitors deployed on the Internet [5]. They also present solutions to make passive Internet threat monitors "harder to detect" [5].

Passive Internet threat monitors are an important tool for obtaining a macroscopic view of malicious activity on the Internet. In the paper, they showed that they are subject to detection attacks that can uncover the location of their sensors. They believe that they have found a new class of Internet threat, because it does not pose a danger to the host systems themselves, but rather a danger to a Meta system that is intended to keep the host systems safe. [5]

Even though they believe that they have not fully well-defined the threat, they presented marking algorithms that work in practice. Passive Internet threat monitors were derived more or less empirically, so it is possible that there may be more efficient marking algorithms that they did not study. For example, methods for detecting remote capture devices has been studied in the context of remote sniffer detection, but none of those studies have correlated plain sniffers with threat monitors and there may be techniques that can be applied in their context. To find insights that they may have missed, a more mathematical approach to the analysis of feedback properties may be necessary. [5]

They presented some techniques to protect against their markings algorithms, but some of those solutions are tough to implement, and others still need to be studied more carefully for their practicality and effectiveness and most importantly, for their vulnerabilities. The goal of their paper is to bring attention of the problem to the research community and leverage people with various expertise’s, not limited to system and network security, to protect of this important technology. Continuing efforts to better understand and protect passive threat monitors are essential for the safety of the Internet. [5]

4. Recommendation and Planning

In the past, the government and private companies did not yet cooperate in terms of protecting the Internet infrastructure from the internet risk, the internet threat and cybercrime. ISPs recognize as the owners of the Internet network in Malaysia [22]. They are the heartbeat of the Malaysian Internet as they interconnect the Malaysian public and private network with the global networks [22]. In this study, we propose that government agencies and the private companies have to collaborate in detecting internet threat within Malaysia. This figure 3 shows the collaborative between MCMC, MyCERT and antivirus company such as Kaspersky and F-Secure. We need to collaborate with the antivirus companies where their labs located in Malaysia, such as Kaspersky and F-Secure. SNSC is the lab that owned by MCMC, the lab has the attack signature database to identify the threat by signature matching. The database needs to update regularly for the purpose of detecting the threats from the internet, but the database of threat owned by MCMC is not enough to detect all the threats in the internet. Therefore, the advancement of antivirus company and MyCERT can help the system to detect more threat effectively. The signature database at SNSC will be updated by three organizations instead of just one organization. This database contents the recent signature of the cyber threats not only from SNSC system but also from antivirus company as an expertise of the cyber threats and MyCERT as a research and development of cyber threats in Malaysia. From this database, the system can do signature matching with the ISPs traffic in and out Malaysia and detect the threat through the internet traffic. Furthermore, the effectiveness of the detection which avoid from false detection can also upgrade the responsiveness of the events or the threats. The SNSC can directly identify which particular website or port which virus or attack is transfer or connected. Then, the system can straightaway inform the ISPs to block particular port or the websites. This collaboration can make a system more powerful and efficient when detecting the recent internet threats and can response faster of new threats. Moreover, this system also can make the government planning to become a true, which is to bring internet a safer place successful.

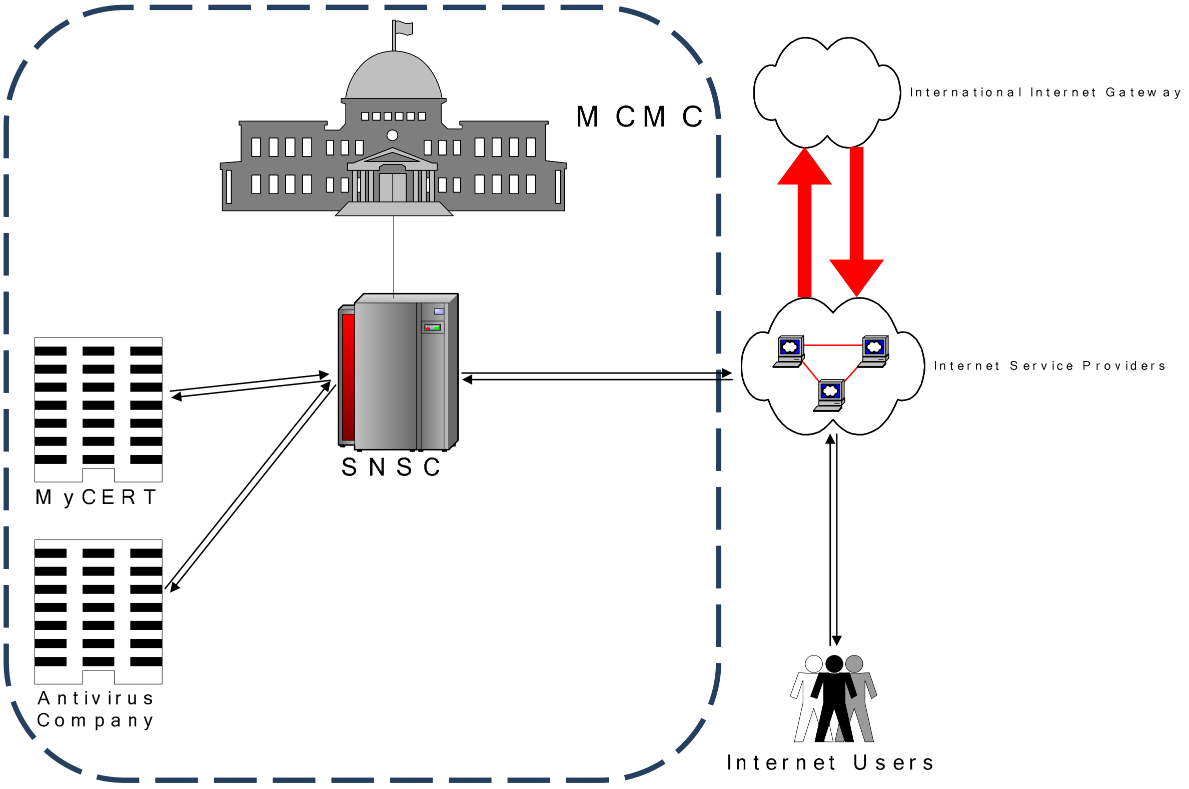

Figure 3.Proposed Collaboration Internet Threat Detection System Model

5. Challenges

Nowadays, the world is connected to a network of information that can be overwhelming. This has produced rapid changes in the global economy and also has an effect to the society and security of the state inevitably. Catherine (The Internet and the Global Economy, 2001) explained that information, the network of the Internet, electronic commerce and the reorganizations associated with the new economy increase the efficiency of resource utilization, which translates into faster productivity growth, which supports higher sustainable GDP. Moreover, IBM XForce mentioned, currently the Internet threat has been increases in a variety of formats [10]. The numbers of Web links that are insecure is more than 500 percent in the first half of the year 2010 [10]. Crime techniques on the cyber space are becoming more sophisticated and creative. This situations can allows Internet users are move vulnerable to become victim to these criminal acts and cannot be limited extent by the government anymore.

The collaboration between the government and relevant private organization is important in order to enhance effective effort in threat prevention. Cooperation can also lead to efficiency in identifying and finding the right solutions, increased capability to discover the new threats and the setting up of preventive measures and can provide updates on the threats to improve responses from all corners of the world. However, it is not easy to collaborate within government agency and private company, as we know that usually the private companies are thinking about earns the profit. Consequently, this idea makes collaborative concept between government and private company is a challenge and it is not easy. Sometimes, private companies want to help the organizations if they were paid. Nevertheless, the collaborative concept needs cooperation from the two sides to work together as a team and have same purposes.

6. Conclusion

Today, we can see that many countries around the world have realized the damage of the cyber threats. This can be seen from the examples of other countries that have been affected by the threats. For example, Cybercriminal groups have significantly enhanced the method to robbery of data [20]. They also try to invent new ways which protection of the network cannot reach it, such as in 2009, use of Malware that protection technologies did not catch the virus example Conficker worm in 2009 [11]. It has become a big problem and many countries have announced that cyber threat is national agenda.

Information security is essential not only for the government but also for all business entities and citizens. At the same time, the information system of a government could be one of the most targeted objects of the malicious activities in the cyber world. The continuous monitoring from the government and preparedness to possible attacks is an imperative. To answer this, there should be a closer cooperation between private companies and the government. The project will improve the role of Governments in this particular area to enhance the operational capabilities of internet networks protection in Malaysia and to increase the quality of the services.

7. References

[1] The White House. (2009). *Remarks by The President on Securing Our Nation'S Cyber Infratructure*. Retrieved from White House website: www.whitehouse.gov

[2] MyCERT. (2010). *MyCERT Incident Statistics*. Retrieved from MyCERT website: www.mycert.org.my

[3] SNSC. (2009). *Info for Home Users*. Retrieved from SKMM website: skmm.gov.my/cybersecurity

[4] MCMC. (2010). *Securing the Network Series 2*. Retrieved from SKMM website: skmm.gov.my

[5] Yoichi Shinoda, ko Ikai, Motomu Iton. (2002). *Vulnerabilities of Passive Internet Threat Monitors.*14th USENIX Security Symposium.

[6] Andrew Schrock and Danah boyd (2008). Berkman Center for Internet & Society Harvard University: *Online Threats to Youth: Solicitation, Harassment and Problematic Content.*

[7] J. Lane Thames, Fandal Ablet (2007). Feorgia Institute of Technology: *Implementing Distributed Internet Security using a Firewall Collaboration Framework.*

[8] E. Skoudis, *Counter Hack: A step by step guide to computer attacks and effective defenses*, Prentice Hall, Upper Saddle River, NJ, 2002.

[9] M.F Abdulla, C.P. Favikumar (2004). *A self-checking signature scheme for checking backdoor security attacks in Internet.* Department of Computer Science, University of Yemen.

[10] *IBM X-Force Threat Reports*. (2010). Retrieved January 25, 2011, from IBM website, www.935.ibm.com

[11] McMillan, Robert. (2009). *Experts bicker over Conficker numbers*", *Techworld* (IDG), retrieved April 23, 2009.

[12] Mary Madden. (2006). Internet Penetration and Impact. Retrieved April 30, 2006, from www.pewinternet.org

[13] John Palfrey & Urs Gasser. (2008). *Born Digital: Understanding the First Generation of Digital Natives.* New York: Basic Books.

[14] Victoria Rideout. (2007). *Parents, Children & Media: A Kaiser Family Foundation Survey.* http://www.kff.org/entmedia/7638.cfm

[15] Gill Valentine. (2004). *Public Space and the Culture of Childhood.* Hants: Ashgate

[16] Justine Cassell & Meg Cramer. (2007). High Tech or High Risk: Moral Panics About Girls Online. In Tara Mcpherson (Ed.), *Macarthur Foundation Series on Digital Media and Learning: Digital Youth, Innovation, and the Unexpected* (pp. 53-75). Cambridge: MIT Press.

[17] Alice Marwick. (2008). *To Catch a Predator? The Myspace Moral Panic.* First Monday, 13(6), article 3.

[18] Jeffrey S. Victor. (1993). *Satanic Panic: The Creation of a Contemporary Legend.* Open Court Publishing Company.

[19] Kulanthaivelu, Saravan. (2010). *Securing The Network 2010 Series 1*. National Cyber Threat Landscape: First Quarter Report. Retrieved from SKMM website: http://skmm.gov.my/cybersecurity

[20] Markoff, John (2009). "*Defying Experts, Rogue Computer Code Still Lurks*". New York Times. Retrieved January 25, 2011, From http://www.nytimes.com/2009/08/27/technology/27compute.html?_r=1

[21] Mann, L. Catherine. (2001). *The Internet and the Global Economy.* Prepared for "Theme 1: Network Economy and Economic Globalization". International Symposium on Network Economy and Economic Governance

[22] MCMC. (2008). MCMC Annual Report 2008. Retrieved from SKMM Website: http://www.skmm.gov.my/link_file/about_us/pdf/Web%20Update%20Annual%20Report/AR_2008.pdf