(IJCSIS) International Journal of Computer Science and Information Security,
Vol. 9, No. 2, February 2011

Behavioral Analysis on IPv4 Malware in both IPv4 and IPv6 Network Environment

Zulkiflee M., Faizal M.A., Mohd Fairuz I. O., Nur Azman A., Shahrin S.
Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka (UTeM), Malacca, Malaysia
zulkiflee@utem.edu.my, faizalabdollah@utem.edu.my, mohdfairuz@utem.edu.my, nura@utem.edu.my, shahrinsahib@utem.edu.my

***Abstract* - Malware is become an epidemic in computer network nowadays. Malware attacks are a significant threat to networks. A conducted survey shows malware attacks may result a huge financial impact. This scenario has become worse when users are migrating to a new environment which is Internet Protocol Version 6. In this paper, a real Nimda worm was released on to further understand the worm behavior in real network traffic. A controlled environment of both IPv4 and IPv6 network were deployed as a testbed for this study. The result between these two scenarios will be analyzed and discussed further in term of the worm behavior. The experiment result shows that even IPv4 malware still can infect the IPv6 network environment without any modification. New detection techniques need to be proposed to remedy this problem swiftly.**

Keywords-IPv6, malware, IDS.

I. INTRODUCTION

IPv6 is a new network protocols which is meant to overcome IPv4 problems. Many advantages offered by this new protocol including 1) A large number of address flexible addressing scheme 2) Offers packet forwarding more efficient 3) Support for secure communication 4) Better support for mobility and many more [1]. Although IPv6 offers a lot of benefits, people are still reluctant to totally migrate from IPv4 to IPv6 network. This is because even IPv6 have been deployed for many years, this protocol is still considered in its infancy [2]. Many researchers have spent ample of time to enhance the IPv6 services to become at least at par with IPv4 addresses. Since IPv4 addresses are facing depletion, migrating to IPv6 is inevitable eventually [3-5]. Some studies claimed that IPv6 cause many security issues [6-9]. Unfortunately, researchers pay little attention on IPv6 security issues[10]. Thus, some culprits are really eager to fully utilities all the vulnerabilities occur during this transition period. Producing malware is one of the most popular techniques to be used. Studies show that new age malwares can survive in new network environment [11, 12]. Hence, researchers agree that further studies have to be conducted to remedy the malware infection issues [13-16].

Malware is software which rapidly invented to manipulate vulnerabilities of computer networks. Based on [17], 250 new malware variants were introduced everyday from all over the world. These so called new age malwares were not new genuine ones but rather innovated from the existing malware. These malwares were modified and some modules were added to it to avoid being detected from the anti-virus software which is using signature patterns to detect malwares.

Malware is become an epidemic in computer network nowadays[18]. Malware attacks are a significant threat to networks. A conducted survey shows malware attacks may result a huge financial impact[19]. This scenario is becoming worse when users are migrating to a new environment which is Internet Protocol Version 6.

The objectives of this study are to determine whether an IPv6 network is totally safe from attacks which were intended for IPv4 network and to identify malware behavior in different network environments.

In the following chapters, we will explain about some related works to this study and followed by the methodology used in this experimental research. The experimental design will be explained and some result and analysis will be discussed. Finally, the conclusion for the overall study will be stated in the end of this paper.

II. RELATED WORK

A. Malware

Malware are represented by several forms namely virus, Trojan, spyware, adware and worms [20, 21]. Each of them has different characteristics to attack their victims. Their method of propagation also varied including sharing memory sticks, downloading files, peer-to-peer applications, sharing file and many more.

B. Malware Propagation Methods

Many activities can help these malware propagate more easily. Unfortunately, most of end-users are not fully aware of it due to lack of knowledge about this issue. We have classified this propagation in two categories namely 1) human intervention and 2) self-propagation.

Most of malware are spreading involving human intervention. These activities including transferring virus via

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

memory sticks, installing peer-to-peer applications, downloading files which contain malware and sending/forwarding malware emails. Malwares fall in this category are virus, Trojan, spyware and adware. Since its propagation based on human intervention, the spreading rate cannot be determined cause the key value of spreading the virus is very subjective. If those malware transferred rapidly by victims, then the spreading rate is very high. However, if it just left without any execution in the computer, the malware will stay dormant and the spreading rate will be low.

The other propagation category is self-propagation. The only malware falls in this category is worm. This is because the spreading method has been pre-defined and hardcoded in the worm software so that it can launch the attack by itself without needed any intervention by human. Worms normally will scan for victims before it initiate the first attack. Therefore, this worm spreading can be determined technically. However, it is not easy to determine it because each of them is using different scanning method to search for their victims.

C. *Malware Scanning Methods*

The worm scanning methods can be divided into three categories as defined by [22] 1) naïve random scanning, 2) sequential scanning and 3) localized scanning. The first scanning method already defined the target regardless the information about the victim's network. The example worm which is using this technique is Slammer. The second scanning method will search for vulnerable hosts through their closeness in IP address space based on host configuration. Blaster worm is an example uses this technique to attack its victim. Finally, the last scanning method preferentially searches for vulnerable hosts in the local subnetwork. It uses the victim's network information to initiate the attack. Nimda worm is an example uses this technique to attack its victim.

We believe the localized scanning method is very dangerous since its will use the information about the current network to launch its attack and the result will be disastrous. What is more, this worm can survive in a new network environment for example in IPv6 network environment. This paper has used Nimda variant E to be released in both IPv4 and IPv6 network environment to see how this worm works and how it will affect the network performance.

III. METHODOLOGY

In this study, we have planned some work flow in order to get our expected result. The methodology used for this study as depicted in the Figure 1.

In order to test the IPv4 worm behavior in both IPv4 and IPv6 network environment two testbeds have been implemented. The computer setup and configuration are identical except for the protocol used to communicate between computers are different. The testbed design for this study can be found in Figure 2.

Before the worm released, a clean testbed need to be ready. Some worms will remain in the memory even after the virus was cleaned by the antivirus software. Therefore, each computer will be cleaned thoroughly including format all computers involve to ensure no other factors will affect the result later on. The original configuration for computers, router and switch involve will be restored.

After the clean testbed ready, the packet sniffer node will be activated to capture all packets through the gateway router. The reason the gateway router involves in this experiment is because to simulate as if this environment is accessible to the other networks. Therefore, this will stimulate the worm to launch its attack to broader scale rather than local area network only.

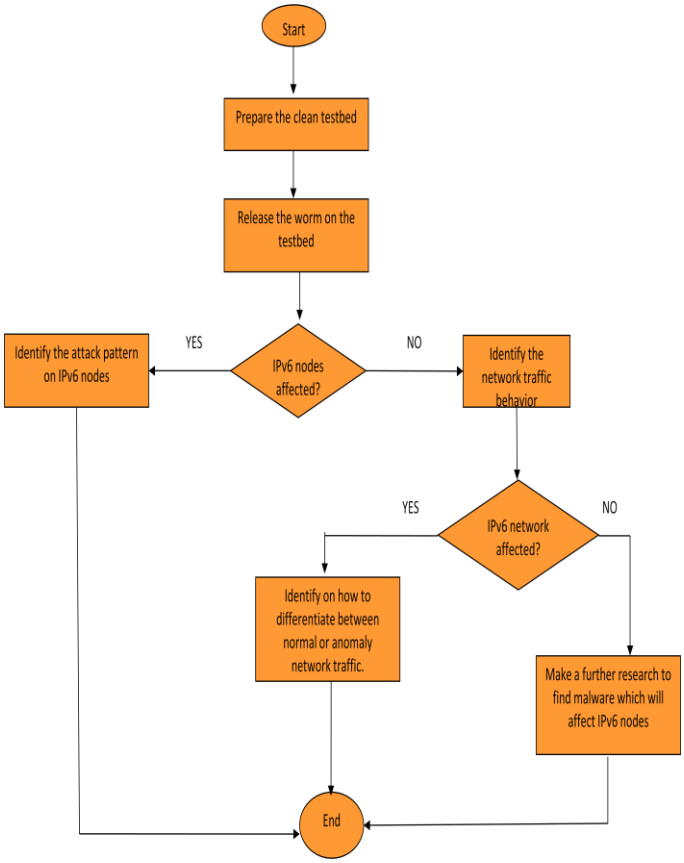

Figure 1: Research Methodology

Since worm in IPv6 is still new, we are expecting two different results will occur based on the worm behavior. The first one, the worm will survive in IPv6 network environment and attack IPv6 nodes directly. If this is the case, then the attack pattern can easily be determined based on changes happened in the affected nodes. However, if the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

worm is not affecting the IPv6 then we will see whether the worm probably affect the network bandwidth. Then, if the worm is consuming the bandwidth consumption, the anomaly pattern needs to be determined later on. Otherwise, the worm can be considered totally dormant in IPv6 network.

IV. Experiment Design

In this experiment, we used the network layout as depict in Figure 2:

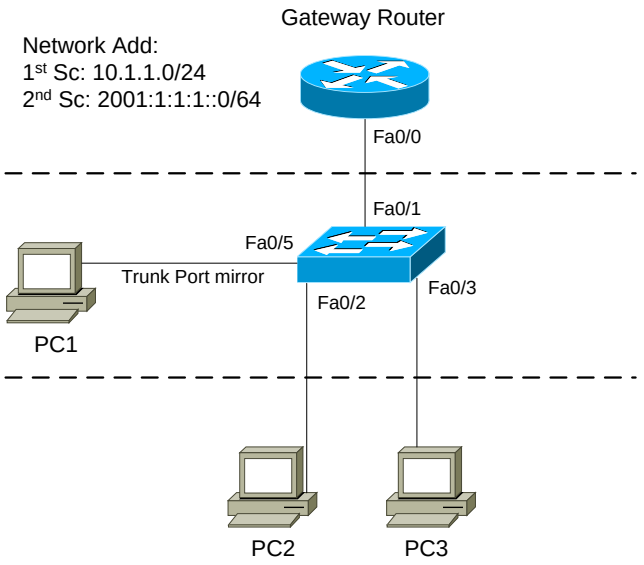

Figure 2: Testbed Network Layout

Based on Figure 2, three computers had been setup in this testbed namely PC1, PC2 and PC3. PC1 was installed a packet sniffer software to capture all traffic through the gateway router trunk. PC2 and PC3 work as nodes in the same network where PC2 as the source who release the worm. These computers used Windows XP SP1 as their operating system and Nimda variant E will be used as the worm in the experiment.

The procedure of this experiment is as the following:

S1: Ready all computers, router and switch. Restore all default configurations into those computers, router and switch.
S2: Activate the packet capture software on PC1 to start capture the ideal network pattern.
S3: Leave the computers for a few minutes to ensure the network traffic has become stable.
S4: Start releases the Nimda.E worm from PC2.
S5: Wait for a few seconds until we can saw the worm started infected the network.
S6: Leave the computer for a few minutes to ensure the worm fully infected the network.
S7: Plug out all cables connected to computer to stop the simulation and save the network traffic log from PC1 for further analysis.
S8: Before starts the next experiment session, all computers must be formatted to ensure it is free from worm infection in operating system and in its memory.

V. Result & Analysis

A. The First Scenario

In this scenario, IPv4 network protocol will be used. The network address used for this scenario is 10.1.1.0/24. Before the worm was released, the ideal network traffic pattern was captured as a benchmark. Figure 3 shows the benchmark of an ideal network traffic pattern.

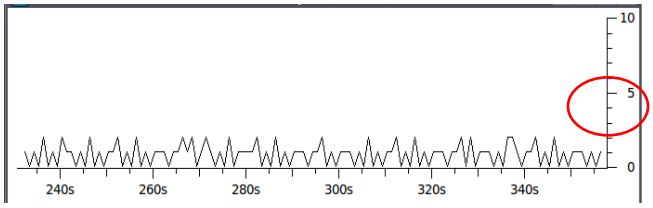

Figure 3: Ideal Network Traffic Pattern for IPv4 network

Figure 3 shows the graph about number of packets captured through the gateway router in seconds. For an ideal network, the traffic through the gateway router interface is less than 3 packets per second as depict in Figure 3. These packets were released for the network information convergence.

After the network stable, the worm was released in the network. After the worm was released, the number of packet received by the gateway router was increased exponentially as depicted in Figure 4. The sample of the captured packet is depicted in Figure 5.

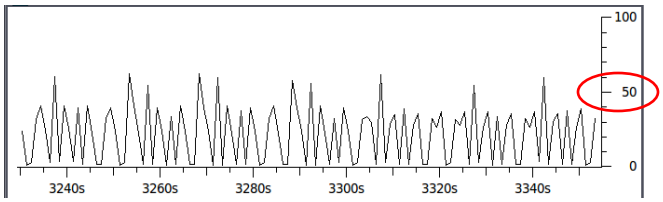

Figure 4: Network Traffic pattern after Nimda.E worm released in IPv4 network

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

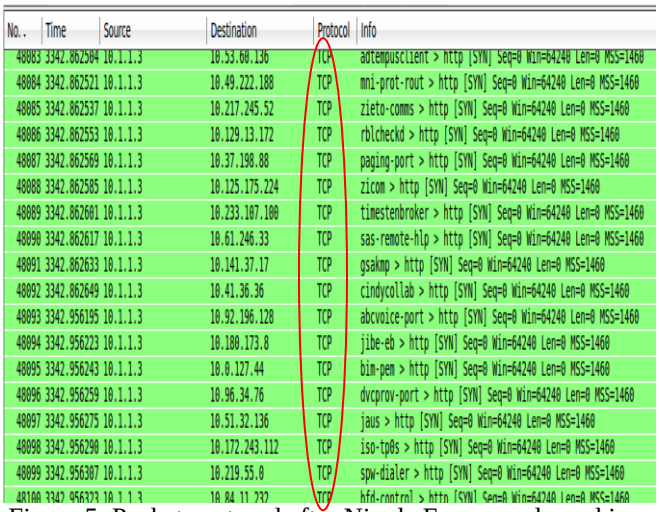

Figure 5: Packet captured after Nimda.E worm released in IPv4 network

Figure 4 shows the graph about number of packets captured through the gateway router in seconds. After the worm was released, it shows that the number of packets through the gateway router was dramatically increased up to almost 55 packets per seconds as depicted in Figure 4. Meanwhile, Figure 5 show the sample of packets captured after the worm was released. It seems that the worm released TCP flooding those packets were generated by one IP address which it is belong to the infected computer based on the IP address. We conclude after a computer was infected by Nimda.E worm, it will release a massive number of TCP connections to connect to its potential victims based on the network address information from the infected computer.

B. The Second Scenario

In this scenario the network layout and the computers setup were identical with the previous scenario. The only different in this scenario was the computers were using IPv6 network protocol instead of IPv4. The network address for this scenario is 2001:1:1:1::0/64. Same as in previous scenario, the ideal network traffic pattern was captured as a benchmark in it is depicted in Figure 6:

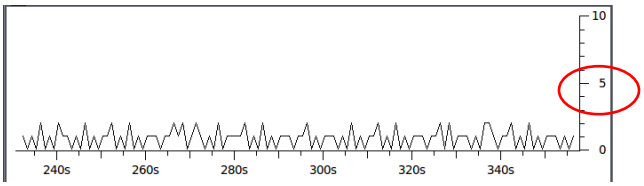

Figure 6: Ideal Network Traffic Pattern for IPv6 network

Figure 6 shows the graph about the number of packet through the gateway router in seconds. Same as in previous scenario, in an ideal network the traffic through the gateway router is less than 3 packets per seconds which were used for the network information convergence.

After the network stable, the worm was released in the network. After the worm was released, the number of packet received by the gateway router was increased exponentially as depicted in Figure 7. The sample of the captured packet is depicted in Figure 8.

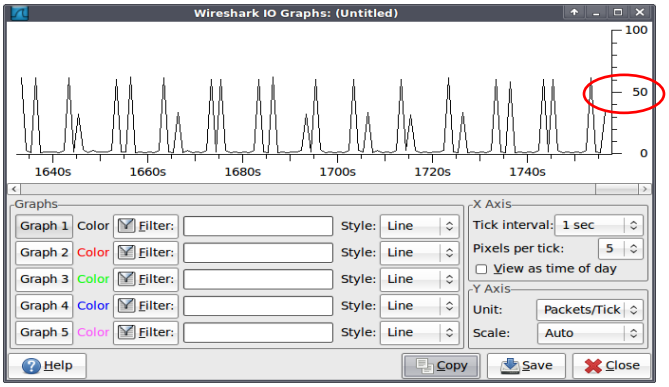

Figure 7: Network Traffic pattern after Nimda.E worm released in IPv6 network

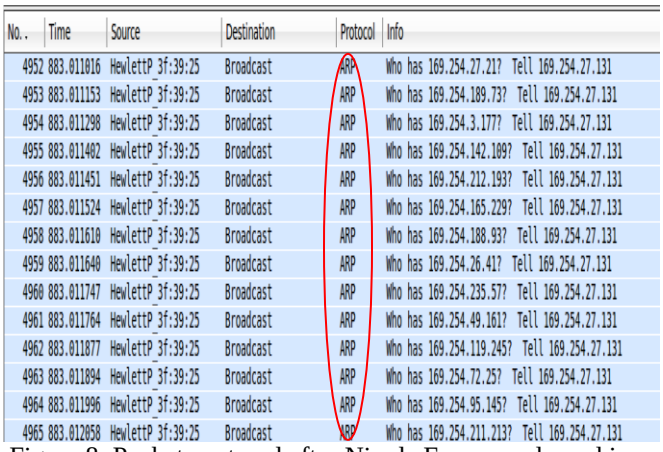

Figure 8: Packet captured after Nimda.E worm released in IPv6 network

Figure 7 shows the graph about number of packets captured through the gateway router in seconds. After the worm was released, the number of packets through the gateway router way severely increased to almost 55 packets per seconds as shown in Figure 7. Figure 8 shows the sample of packets captured after the worm was released. If in IPv4, the worm released the TCP flooding but in IPv6 it released ARP flooding instead. We believe this is because the worm was trying to attack its victim in IPv4 network even the worm was released in IPv6 network environment. We realized the infected computer is not using

C. The Experiment Result Analysis

After all the experiments done, we gathered all the information for further analysis. Figure 9 shows the comparison between numbers of packet released based on different scenarios.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

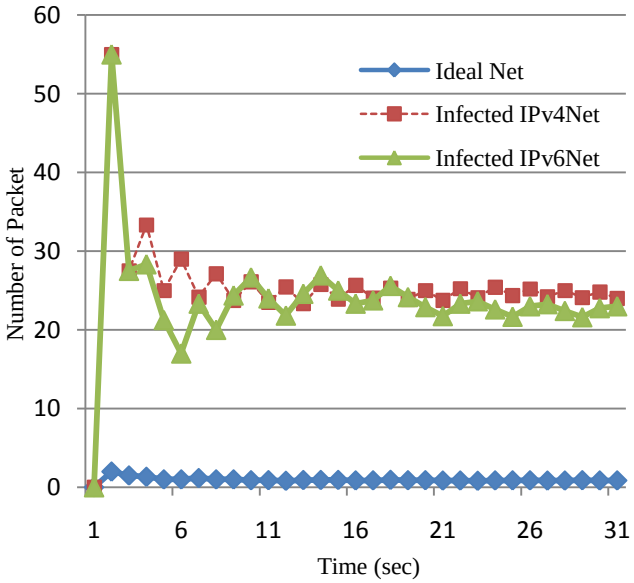

Figure 9: The average packet released based on different scenarios

Figure 9 shows the comparison of numbers of packets released based on three different scenarios. The first line is about the average number of packets released in second after the worm infected in IPv4 network. The second line is about the average number of packets released in second after the worm infected in IPv6 network. The last line is about the average number of packets released on an ideal network. Since the number of packet released in ideal network are identical between IPv4 and IPv6 network, then this information is represented by one scenario only.

From the Figure 9, we can see that the numbers of packets are exponentially increased after the worm was released compares to an ideal network regardless the network protocol used whether it is in IPv4 or IPv6 protocol. However, the number of packets released in IPv4 is slightly higher compares in IPv6 and the type of packets released in each network are also different. This is probably because the router need more time to process the address information in IPv6 due to its long ip addressing scheme. Moreover, the type of packet released was also different in IPv4 compares to IPv6 where in IPv4 the worm was released TCP connections to its victim whereby in IPv6 the worm was released ARP packet to connect to its victim as depicted in Figure 5 and Figure 8. The comparison is compiled in Table 1.

Table 1: Comparison Between Different Scenarios

	Ideal Network	**Infected IPv4 Net**	**Infected IPv6 Net**
Maximum number of packets released (per sec)	3	55	55
Average packet released per second	Low	Slightly Higher	High
Type of packet	Network Discovery	ND & TCP	ND & ARP
	(ND)		
Type of attack	None	TCP Flooding	ARP Flooding

D. *The Experiment Findings*

After two different scenarios executed and analyzed, we compiled our conclusions for this study as the following:

- Even IPv6 node infected, it still look for its victim in IPv4 network. This shows that IPv4 malware still can survive in IPv6 network environment without any modification made on the existing worm.

- In IPv4 network, the nimda worm will release TCP flooding attacks whereas in IPv6 network, the worm will behave differently by releasing ARP flooding attacks.

- IPv4 worm will not directly infect the IPv6 nodes, but it will totally consume the IPv6 network. IPv6 seem not totally invincible from attack even the attack was intended for IPv4 network. This scenario will become worse if the network is using transition mechanism to communicate between IPv4 and IPv6 network protocol.

VI. CONCLUSION

Migrating from IPv4 to IPv6 is inevitable. Many researchers put a lot of effort to ensure the IPv6 services and stability to be much better compares to IPv4. However, not many researchers pay enough attention on security issues. The malware give severe impact on the network which cause a lot of trouble to end users. This paper shows that malware which was invented for IPv4 network still can penetrate and survive in IPv6 network without any modification made on the existing malware. This issue will be worse if the organization is using transition mechanism to communicate both their IPv4 and IPv6 nodes.

For further research, a more realistic testbed need to be used to represent the real network environment. A study on how this worm behaves in transition mechanism such as dual-stack need to be conducted to further understand how it works. Finally, a new detection technique needs to be proposed to cater this issue.

VII. ACKNOWLEDGEMENTS

The research presented in this paper is supported by Malaysian government scholarship and it was conducted in Faculty of Information and Communication Technology (FTMK) at University of Technical Malaysia Malacca (UTeM).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VIII. REFERENCES

[1] Waddington, D.G. and F. Chang, *Realizing the transition to IPv6.* IEEE Communications Magazine, 2002. **40**(6): p. 138-147.

[2] Ismail, M.N. and Z.Z. Abidin. *Implementing of IPv6 Protocol Environment at University of Kuala Lumpur: Measurement of IPv6 and IPv4 Performance*. in *Future Computer and Communication, 2009. ICFCC 2009. International Conference on*. 2009.

[3] Zheng, Q., T. Liu, X. Guan, Y. Qu, and N. Wang, *A new worm exploiting IPv4-IPv6 dual-stack networks*, in *Proceedings of the 2007 ACM workshop on Recurring malcode*. 2007, ACM: Alexandria, Virginia, USA.

[4] Hua, N. *IPv6 test-bed networks and R&D in China*. in *Applications and the Internet Workshops, 2004. SAINT 2004 Workshops. 2004 International Symposium on*. 2004.

[5] Kamra, A., H. Feng, V. Misra, and A.D. Keromytis. *The effect of DNS delays on worm propagation in an IPv6 Internet*. in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*. 2005.

[6] Badamchizadeh, M.A. and A.A. Chianeh. *Security in IPv6*. in *Proceedings of the 5th WSEAS International Conference on Signal Processing*. 2006. Istanbul, Turkey.

[7] Warfield, M.H., *Security Implications of IPv6.* Retrieved April, 2003. **30**: p. 2006.

[8] Sharma, V., *IPv6 and IPv4 Security challenge Analysis and Best-Practice Scenario.* International Journal of Advanced of Networking and Applications, 2010. **01**(04): p. 258-269.

[9] Yuce, E., *A CASE STUDY ON THE SECURITY OF IPV6 TRANSITION METHODS.* ACM Workshop on Recurring Malcode, 2009.

[10] Zhao-wen, L.I.N., W. Lu-hua, and M.A. Yan, *Possible Attacks based on IPv6 Features and Its Detection.* Network Research Workshop, APAN, 2007.

[11] Gold, S., *The changing face of malware.* Computer Fraud & Security, 2009. **2009**(9): p. 12-14.

[12] de la Cuadra, F., *The geneology of malware.* Network Security, 2007. **2007**(4): p. 17-20.

[13] Hansman, S. and R. Hunt, *A taxonomy of network and computer attacks.* Computers & Security, 2005. **24**(1): p. 31-43.

[14] Bellovin, S.M., B. Cheswick, and A.D. Keromytis, *Worm propagation strategies in an IPv6 Internet.* LOGIN: The USENIX Magazine, 2006. **31**(1): p. 70-76.

[15] Zagar, D., K. Grgic, and S. Rimac-Drlje, *Security aspects in IPv6 networks-implementation and testing.* Computers & Electrical Engineering, 2007. **33**(5-6): p. 425-437.

[16] Jordan, C., A. Chang, and K. Luo. *Network Malware Capture*. 2009: IEEE Computer Society.

[17] Stewart, J., *Behavioural malware analysis using sandnets.* Computer Fraud & Security, 2006. **2006**(12): p. 4-6.

[18] Lelarge, M. *Economics of malware: Epidemic risks model, network externalities and incentives*. in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*. 2009.

[19] Computer Economics, *Annual Worldwide Economic Damages from Malware Exceed $13 Billion*. 2007.

[20] Karresand, M., *A proposed taxonomy of software weapons.* No. FOI, 2002.

[21] Robiah, Y., S.S. Rahayu, M.M. Zaki, S. Shahrin, M.A. Faizal, and R. Marliza, *A New Generic Taxonomy on Hybrid Malware Detection Technique.* Arxiv preprint arXiv:0909.4860, 2009.

[22] Chen, Z. and C. Ji, *An information-theoretic view of network-aware malware attacks.* 2008.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500