AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Detecting Worm Attacks in Cloud Computing Environment: Proof of Concept

[1]Hasan Mahmoud Kanaker, [1]Dr. Madihah Binti Mohd Saudi, [2]Dr. Mohd Fadzli Marhusin

[1]*Faculty of Science and Technology Universiti Sains Islam Malaysia (USIM) Bandar Baru Nilai, Malaysia.*
[2]*Universiti Sains Islam Malaysia (USIM) Bandar Baru Nilai, Malaysia .*

ARTICLE INFO

Article history:
Received 8 August 2014
Received in revised form
12 September 2014
Accepted 25 September 2014
Available online 2 November 2014

Keywords:
Cloud computing, Worm Attacks, Detection, Reverse Engineering, Dynamic Analysis.

ABSTRACT

Cloud computing technology is a concept of providing dramatically scalable and virtualized resources, bandwidth, software and hardware on demand to users. Users can request cloud services via a web browser or web service. Cloud computing consists of valuable resources, such as, networks, servers, applications, storage and services with a shared network. By using cloud computing, users can save cost of hardware deployment, software licenses and system maintenance. Many security risks such as worm can interrupt cloud computing services; damage the spiteful service, application or virtual in the cloud structure. Nowadays the worm attacks are becoming more sophisticated and intelligent, makes it is harder to be detected than before. Based on the implications posed by this worm, this is the urge where this research comes in. This paper aims to build a new model to detect worm attacks in cloud computing environment based on worm signature extraction and features behavioral using dynamic analysis. Furthermore this paper presents a proof of concept on how the worm works and discusses the future challenges and the ongoing research to detect worm attacks in cloud computing efficiently.

To Cite This Article: Hasan Mahmoud Kanaker, Dr. Madihah Binti Mohd Saudi, Dr. Mohd Fadzli Marhusin, Detecting Worm Attacks in Cloud Computing Environment: Proof of Concept. ***Aust. J. Basic & Appl. Sci.,*** *8(16): 120-124, 2014*

INTRODUCTION

Cloud computing is a technology that involves a large number of computers connected through Internet or it is a distributed computing over a network. This technology consists of large database, services, applications, software and resources. It has the ability to run a program or applications on many connected computers at the same time and it allows the users to access applications and resources through Internet anytime and anywhere. It provides optimized and efficient computing also has become the next logical step for the IT industry. It's the new strategic in enterprise computing and the new standard in every sector of society, businesses, educational institutions, community organizations (Voas, 2013). Cloud computing technology changed lives of people and improved their work lives through using large a variety of cloud service. Individual's lives are affected by this technology through free email servers, applications and storage capabilities.

Although the cloud computing offers a great deal of benefits, such as, cost reduction, dynamic virtualized resources, store large amount of data and improved productivity (Qaisar & Khawaja, 2012), but at the same time it has many security risks. There are many kinds of possible attacks, such as, denial-of-service (DoS) attack, authentication attack, man-in-the middle attack and worms injection attack (Zunnurhain & Vrbsky, 2010).

Recently, worm has significantly increased its negative influence and has created a drastic chaos in the world of computer and in the cloud computing environment. In terms of cloud worm injection attack, the attacker tries to damage a spiteful service, application or virtual machine in the cloud structure and posed itself as an authorized user and generates its personal spiteful service, application or virtual machine, and implements his malicious code into the cloud structure (Biedermann & Katzenbeisser, 2011).Furthermore, Signature based antivirus can detect very high accuracy when the Signature has been known, the weakness this type of detection is that when the malware change its Signature completely. Commonly, this type of antivirus would fail to detect a novel attack.

The objectives of this research paper are to investigate and to conduct an in-depth study of the worms attack implications in cloud computing environment and to do the proof of concept (POC) testing to see how the worm attacks in cloud computing environment works. From the POC findings, a worm attacks taxonomy and detection

Corresponding Author: Hasan Mahmoud Kanaker, Faculty of Science and Technology Universiti Sains Islam Malaysia (USIM) Bandar Baru Nilai, Malaysia
E-mail: hasankanaker@gmail.com

algorithm will be developed. Later these will be used as the basis to produce an effective model to detect worm attacks in cloud computing environment.

Literature review:

Cloud computing has become popular since it is being introduced in October 2007, and still attracting many researchers. It is a new computing technique under the partnership of IBM and Google (Naone, 2007), (Reimer,2007). Cloud computing uses internet and remote servers for maintaining data and applications. It helps users to minimize usage of hardware, software license and maintaining system. By using Internet, users are able to use services applications on clouds (Hatem, Wafy & El-Khouly, 2014),(Ren & Lou, 2009). Moreover, by using cloud computing, users can access to services quickly and can access broad network. However, apart from the above benefits, cloud computing is prone to vulnerabilities, which includes attacks from intruders. Cloud computing endures lot of security threats, and worm injection attacks is one of the serious concern (Qaisar & Khawaja, 2012), (Zunnurhain & Vrbsky, 2010).

Table 1: The Challenges of Different Worm Detection Methods.

Title	Method used for Worm Detection	Challenges For Improvement
Cloud Computing: Network/Security Threats and Countermeasures (Qaisar & Khawaja, 2012)	- check the authenticity for received messages. - store the original image file using hash function.	-Attacker can create a legitimate hash value to deal with cloud system
Security Attacks and Solutions in Clouds (Zunnurhain & Vrbsky, 2010).	-Using File Allocation Table (FAT). technique. -Utilize the Hyper. visor method -Storing the OS type of the user.	- Process time for the cloud provider is very high.
Retrospective Detection of Malware Attacks by Cloud Computing (Liu & Chen, 2010)	-Portable Executable (PE) format file relationships. -Map Reduce job. -Hadoop platform. -File indexing. -File-relation index.	-These methods only effective on Hadoop platform -Some worms can generate different log file each time so can't detected easily-Process time is high due large number of files. -Detection method based on behavior only.

Based on all the previous works discussed above, the main challenges that should be considered thoroughly are the dataset types and volume, analysis and detection techniques and feature selection to detect the worm attacks in cloud computing environment efficiently.

Therefore, in this research, a new worm detection technique by dynamic analysis and by using bigger and standard dataset and response algorithm will be developed which lead to the formation of a new model to detect worm attacks in cloud computing environment and response. It is expected this new model, will produced a better accuracy rate and lower false negative rates, but will not be discussed in this research paper.

Methodology:

The reverse engineering activities are done in controlled lab environment as shown on Figure 1. It is a controlled lab environment and almost 80% of the software used in this testing is an open source or available on a free basis as displayed in Table 2. No outgoing network connection is allowed for this architecture. The dataset in this research consists of different types of worm and executable files which is downloaded from VX Heaven (VX Heaven, 2014) and Offensive Computing (Offensive Computing, 2014). Many studies have used these dataset in their experiment (Dai, Guha & Lee, 2009), (Saudi, 2011), (Moskovitch, Stopel, Feher, Nissim, Japkowicz & Elovici, 2008), (Khan, Mirza & Khayam, 2010), (AbuZaid, 2013). In these datasets there are many variant of malwares and benign files. There are more than 2400 samples available to be downloadable from this project. These dataset were categorized into different types, which are the BAT, JS, VBS and WIN32. This dataset has been used as the basis of this research testing. The methodology used includes the dynamic analysis in a controlled lab environment.

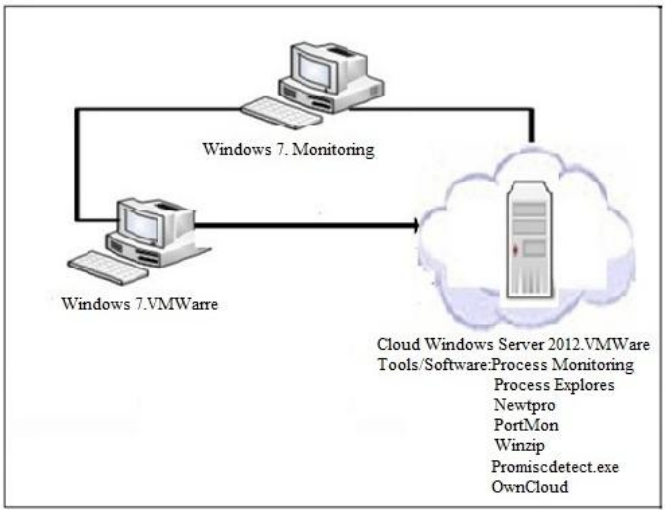

Fig. 1: Controlled Laboratory Architecture.

Table 2: Software Used In The Testing.

Software	Function
VMWare	To build up virtual operating systems in a Computer.
Process monitoring	To conduct the dynamic analysis
Process Explorer	To conduct the dynamic analysis
PortMon	To conduct the dynamic analysis
Newt pro	To conduct the dynamic analysis
Promiscdetect.exe	To conduct the dynamic analysis
Wireshark	To monitor the network traffic generated from the infected computer
Winzip	To unzip compressed file
Own Cloud	To conduct Cloud Server

The mechanism of the dynamic analysis includes executing the worm and observing its actions analysis. The worm attack is activated in a controlled laboratory environment. The dynamic analyses are implemented as illustrated in Figure 2.

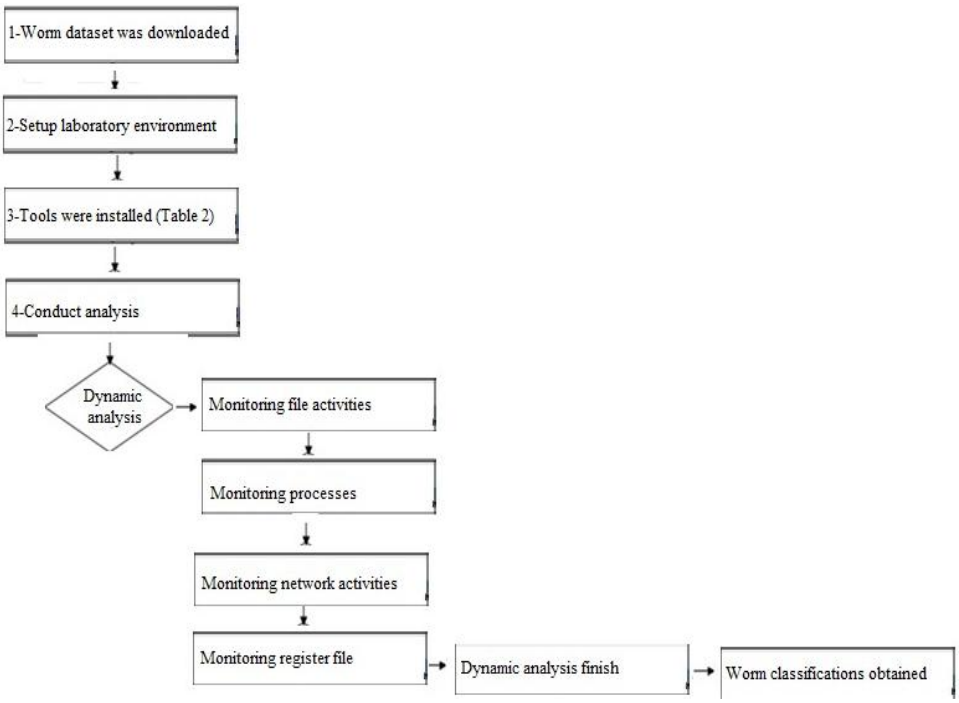

Fig. 2: Dynamic Analysis process

Australian Journal of Basic and Applied Sciences, 8(16) October 2014, Pages: 120-124

Results:

A case study using a sample from Offensive Computing (Offensive Computing, 2014) shows the proof of concept how the worm attack works in cloud computing environment and observe its actions. The architecture used for this testing is the same as in Figure 1, which was conducted in controlled lab environment and by using dynamic analysis and by using the tools listed in Table 2.

Based on the testing conducted, the result showed that the worm dropped a file in C directory as the following and can be referred in Figure 3

C:Windows\System32\Worm64.dll

This file Worm64.dll was used by the worm to attack the cloud server. It damages the files, registry and all data that stored in the server. Then the attacker can access the cloud server and application via the victim's interface such as a web browser. Based on this payload and the testing conducted, it shows that the cloud can be exploited and attacked by a worm

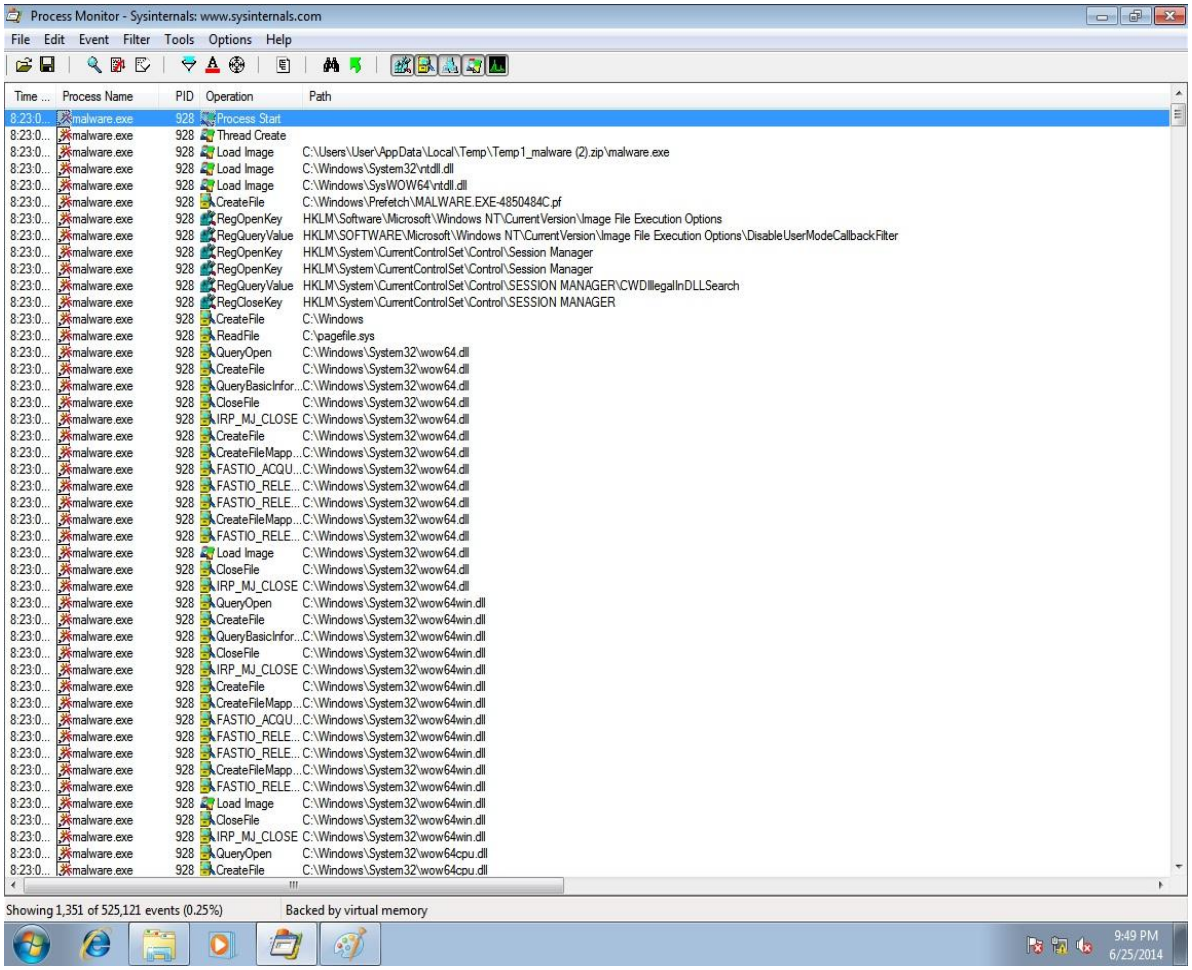

Fig. 3: Screenshots after infected worm malicious.

Therefore, in this paper, the researchers would like to point out some interesting idea for further discussion based on the payload identified. The researchers are proposing to build up worm classification in cloud computing based on the worm payload prior the formation of the worm detection method for cloud computing environment. The proposed model of this idea as displayed in Figure 4. Not much existing research papers related with worm classification in cloud computing have been discussed as the time this paper is written.

Conclusion and future work:

A worm attacks in cloud is an emerging threat and is seen as one of the main threats in cyber world. In this research paper a proof of concept on how worm attacks in cloud has been demonstrated. The payload identified in the POC will be used as the basis of the worm detection model in cloud computing. This paper is part of a larger research project to confront the worm attacks in cloud computing environment. Ongoing research includes producing worm classification and worm detection model for cloud computing environment.

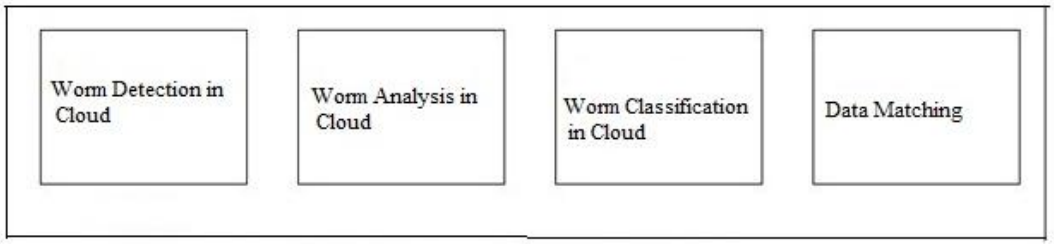

Fig. 4: Worm Detection in Cloud Computing Framework

ACKNOWLEDGMENT

The authors would like to express their gratitude to Universiti Sains Islam Malaysia (USIM) for the support and facilities provided. This research paper is supported by Universiti Sains Islam Malaysia (USIM) grant.

REFERENCES

Voas, J., 2013. Cloud Computing (4): 12–14.

Qaisar, S., K. Khawaja, 2012. Cloud Computing: Network/Security Threats and Countermeasures. Interdisciplinary Journal of Contemporary Research In, pp: 1323-1329.

Zunnurhain, K., S. Vrbsky, 2010. Security Attacks and Solutions in Clouds.

Biedermann, S., S. Katzenbeisser, 2011. *Detecting computer Worms In the cloud*. In Proceedings of the 2011 IFIP WG11.4 International conference on Open Problems in Network Security, pp: 43–54.

Naone, E., 2007. Computer in the Cloud. Technology Review (124, 2012) from http://www.thecnologyreview.com/printerfriendly Article.aspx?id=19397.

Reimer, J., 2007. Dreaming in the Cloud XIOS web operating system. Retrieved (124, 2012) from http://arstechnica.com/news.ars/post/20070408dreamingin the cloud with the xios web operating system.html.

Hatem,S., M. Wafy, M. El-Khouly, 2014. Malware Detection in Cloud Computing. International Journal of Advanced Computer Science and Applications, 5(4).

Ren , K., W. Lou, 2009. Ensuring Data Storage Security in Cloud Computing. Retrieved From http://www.ece.iit.edu/~ubisec/IWQoS09.pdf.

Liu, S., Y. Chen, 2010. Retrospective Detection of Malware Attacks by Cloud Computing. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, pp: 510–517.

VX., Heaven, 2014, Computer Virus Collection, URL: http://vxheaven.org/vl.php.

Offensive Computing, 2014. Malware Search, URL: http://www.offensivecomputing.net.

Dai, J., R. Guha, J. Lee , 2009. Efficient Virus Detection Using Dynamic Instruction Sequences. Journal of Computers, 4(5): 405-414.

Saudi, M., 2011. A New Model for Worm Detection and Response (PHD thesis), University of Bradford, United Kingdom.

Moskovitch, R., D. Stopel, C. Feher, N. Nissim, N. Japkowicz, Y. Elovici, 2008. Un- known malcode detection and the imbalance problem. Journal in Computer Virology Volume 5, Number 4: 295-308.

Khan, H., F. Mirza, S. Khayam, 2010. Determining malicious executable distinguishing attributes and low-complexity detection. Journal In Computer Virology, 7(2): 95-105.

Abu Zaid, A., 2013. An Efficient Trojan Horse Classification (ETC), IJCSI International Journal of Computer Science Issues, 10, 2(3), March 2013, ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784.