'ULŪM ISLĀMIYYAH JOURNAL VOL.13 (SPECIAL EDITION) 2014 : pp 129-143
ISSN 1675 - 5936 I e-ISSN 2289-4799
UNIVERSITI SAINS ISLAM MALAYSIA

A New Model for Trojan Detection using Machine Learning Inspired by Al-Furqan Verse

Madihah Mohd Saudi[1] & Areej Mustafa Abuzaid
Universiti Sains Islam Malaysia

Masrur Ibrahim
Institut Pendidikan Guru, Kampus Pendidikan Islam

Abstract

Living in a cyber-world, it is becoming very common for users to receive lots of emails with different files attachment. Sometimes some of the files might contain malicious file. It is not an easy job to differentiate between benign and malicious file in the email attachment without the help of the anti-virus. Worse than that many game applications can be downloaded free from many websites and it might contain malicious file as well. In Quran, surah Al-Furqan, verse 53 (25:53) stated that how Allah, the all Mighty has made a barrier and inviolable obstruction so that two seas can flow freely. The seas were partition as palatable and sweet while the other was salt and bitter. When the meaning of this verse is mapped into current cyber world, obviously when dealing with malwares and normal file, a scientific way and an experimental design need to be carried out to differentiate between these two files. Trojan horse is an example of malicious file and it has become a real threat for computer users for more than a decade. It has caused loss lots of money and productivity and it considered as one of the most serious threats in cyber security. The Trojan polymorphism characteristics make the detection processes much harder than before. Therefore, in this research paper, a new model called ETDMo (Efficient Trojan detection model) is built to detect Trojan horse more efficiently. The static, dynamic and automated analyses have been conducted. Moreover, the knowledge discovery techniques (KDD) and the data mining algorithm were used to optimize the accuracy result. Based on the experiment conducted, this ETDMo model produces an overall accuracy rate of 98.2% with 1.7% for false positive rate.

Keywords: Trojan horse, classification, payload, static analysis, dynamic analysis, automated analysis, Al-Furqan verse 53.

1 Corresponding author : Madihah Mohd Saudi, Faculty of Science and Technology, Universiti Sains Islam Malaysia, e-mail : madihah@usim.edu.my

INTRODUCTION

Nowadays there are many scenario where the end users are having hard time to detect between a malicious file and non-malicious file especially when downloading any application or file from the website. In the year of 2013, the Australia Computer Emergency Response Centre (AuSCERT) reported that 7,962 cases of the compromised Australia web sites were serving malwares (AuSCERT, 2013). Even worst, statistics taken from Cyber Security, Malaysia (refer Fig. 1) show that malicious code contributes as the most reported with 52 percentages. Trojan horse has been identified as part of the malicious codes.

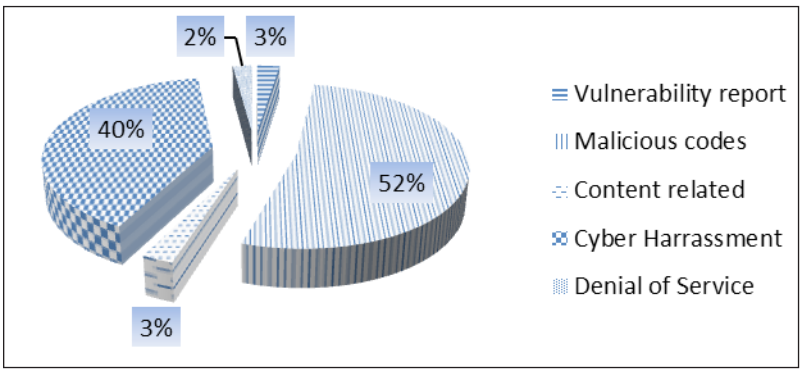

Fig.1. Incident Statistics 2014 (Adapted from Cyber Security Malaysia Incident Statistics (2014))

In this research paper, inspired by surah Al-Furqan, verse 53 (25:53), a new model has been proposed to detect the malicious file specifically the Trojan horse.

وَهُوَ ٱلَّذِى مَرَجَ ٱلْبَحْرَيْنِ هَٰذَا عَذْبٌ فُرَاتٌ وَهَٰذَا مِلْحٌ أُجَاجٌ
وَجَعَلَ بَيْنَهُمَا بَرْزَخًا وَحِجْرًا مَّحْجُورًا ﴿٥٣﴾

Translation: And it is He who has released [simultaneously] the two seas, one fresh and sweet and one salty and bitter, and He placed between them a barrier and prohibiting partition.

The above verse clearly stated how Allah has made a barrier and inviolable obstruction to separate the two seas. When this verse is clearly understood and being applied and mapped into cyber security world, it is a need for the researcher to carry out an experimental design or a scientific way on how to identify and differentiate between a malware and a normal file or application.

In this research paper, the researchers are focusing on Trojan Horse detection method. The whole paper is focusing the experimental way how the Trojan horse is detected. In Table 2 under Finding Section, is the summarization how the Al-Furqan verse is mapped with this research paper.

Trojan horse has become a real threat to many organizations and computer users for more than a decade. Hill (McGraw, 2000) defined malware as any code added, changed or removed from a software system in order to intentionally cause harm or subvert the intended function of the system. Though the problem of malware has a long history, a number of recent, widely publicized attacks and certain economic trends suggest that malware is rapidly becoming a critical problem for industry, government, and individuals. One of the categorizations of the malware is known as Trojan horse, which is the focus of this research paper. It is a malicious program, that must be executed in victim's computer and once it is installed, it can control the victim's computer remotely and steal any confidential information from it. It is different compared to worm and virus, since it has the capability to control the victim's computer remotely and it does not replicate itself (Saudi, 2008).

As for the malware detection, classification is one of the crucial processes that must be place in order to ensure the effectiveness of the detection process. Generally malware can be classified based on the characteristics such as infection target and technique and other different characteristics (Babak *et al*., 2011). An effective classification algorithm or technique can improve the accuracy of malware detection (Nguyen *et al*., 2012). Classification method has been widely used in malicious code analysis especially in measuring the effectiveness of detection for a new or unknown sample of malicious code (Karbalaie *et al*., 2012).

In this paper, a trojan horse classification called an Efficient Trojan Classification(ETC) is developed as a part and basis of a new trojan horse detection model, but the model will not be discussed in this paper.The details on how the ETC is developed are explained in this paper. Hopefully this new ETC can be used as a basis model and guidance to produce a system either to detect or protect organization from Trojan horse attacks.

This paper is organised as follows. Section 2 presents the related works with trojan horse detection techniques,classification and architecture. Section 3 explains the methodology used in this research paper which consists of static and dynamic analyses and the architecture of the controlled laboratory environment. Section 4 presents the research findings which consists of a new trojan horse classification called Efficient Trojan Classification (ETC)

and section 5 discusses the testing and evaluation of the proposed trojan horse classification. Section 5 concludes and summarises the future work of this research paper.

RELATED WORKS

Apart from surah Al-Furqan, verse 53 (25:53), there are many Quranic verses can be used as guidance in our daily life especially when encountering with cyber threat and some of these are referring to natural phenomena. The following are examples of the Quranic verses that are related with computer security field. The interpretation for each Quranic verses in computer security field is summarized as in Table 1.

In Universiti Sains Islam Malaysia (USIM), the method and the level of the integration between Naqli and Aqli knowledge consists of four different level of method (*Mustawa*), which are *M1 -Mustawa Al-Tansis* (How Quranic verses is mapped in certain field or known as *ayatisation), M2- Mustawa Al-Muqaranah (*Comparison*), M3 – Mustawa Al-Taqyim (*Adaptation*) and M4 – Mustawa Al-Tawfiq (*Integration*)*. In this research paper, *M1* has been used as basis for the integration of the Naqli and Aqli knowledge where we are referring to the primary sources of Islamic Sciences and knowledge that are from Al-Quran, al-hadith and the authentic classical Islamic books.

Table 1. Quranic Verses Mapped Into Computer Security Field

Quran verses	Translation	Verses	Relations
وَإِذَا قُرِئَ الْقُرْآنُ فَاسْتَمِعُوا لَهُ وَأَنصِتُوا لَعَلَّكُمْ تُرْحَمُونَ	And when the Quran is recited, give ear to it and pay heed , that ye may obtain mercy .	A'raaf : 7 : 204	Boost immune system by listening to Quran. Therefore it is a need to be alert when there is symptom to trigger any cyber threat.

وَلَقَدْ ذَرَأْنَا لِجَهَنَّمَ كَثِيراً مِّنَ الْجِنِّ وَالإِنسِ لَهُمْ قُلُوبٌ لاَّ يَفْقَهُونَ بِهَا وَلَهُمْ أَعْيُنٌ لاَّ يُبْصِرُونَ بِهَا وَلَهُمْ آذَانٌ لاَّ يَسْمَعُونَ بِهَا أُوْلَـئِكَ كَالأَنْعَامِ بَلْ هُمْ أَضَلُّ أُوْلَـئِكَ هُمُ الْغَافِلُونَ	Already have We urged unto hell many of the jinn and human kind , having hearts wherewith they understand not , and having eyes wherewith they see not , and having ears wherewith they hear not . These are as the cattle nay, but they are worse! These are the neglectful.	A'raaf : 7 : 179	They are various types of virus that have been created which can cause problem to the computer security. Each virus has their own function and threat. That is why it is a need to identify the virus clearly to solve the problem.
وَقَالُوا قُلُوبُنَا فِي أَكِنَّةٍ مِّمَّا تَدْعُونَا إِلَيْهِ وَفِي آذَانِنَا وَقْرٌ وَمِن بَيْنِنَا وَبَيْنِكَ حِجَابٌ فَاعْمَلْ إِنَّنَا عَامِلُونَ	And they say : Our hearts are protected from that unto which thou (O Muhammad) callest us , and in our ears there is a deafness , and between us and thee there is a veil . Act , then we also shall be acting .	Fussilat : 41 : 5	There is a barrier or it represents as the malicious program are trying to enter the computer and they are trying to get pass the barrier. So it advisable to enhance the barrier and security to prevent the malicious program.
وَجَحَدُوا بِهَا وَاسْتَيْقَنَتْهَا أَنفُسُهُمْ ظُلْماً وَعُلُوّاً فَانظُرْ كَيْفَ كَانَ عَاقِبَةُ الْمُفْسِدِينَ	And they denied them , though their souls acknowledged them , for spite and arrogance . Then see the nature of the consequence for the wrong doers!	An-Naml : 27 : 14	If user is being ignorance, the virus or any malicious program will be inside her computer. By only then user can only see the consequences as user did not take precaution.

إِنَّ فِي خَلْقِ السَّمَاوَاتِ وَالأَرْضِ وَاخْتِلاَفِ اللَّيْلِ وَالنَّهَارِ وَالْفُلْكِ الَّتِي تَجْرِي فِي الْبَحْرِ بِمَا يَنفَعُ النَّاسَ وَمَا أَنزَلَ اللَّهُ مِنَ السَّمَاءِ مِن مَّاء فَأَحْيَا بِهِ الأَرْضَ بَعْدَ مَوْتِهَا وَبَثَّ فِيهَا مِن كُلِّ دَآبَّةٍ وَتَصْرِيفِ الرِّيَاحِ وَالسَّحَابِ الْمُسَخَّرِ بَيْنَ السَّمَاء وَالأَرْضِ لآيَاتٍ لِّقَوْمٍ يَعْقِلُونَ	In the creation of the heavens and the earth , and the difference of night and day , and the ships which run upon the sea with that which is of use to men , and the water which Allah sendeth down from the sky , thereby reviving the earth after its death , and dispersing all kinds of beasts therein , and (in) the ordinance of the winds , and the clouds obedient between heaven and earth : are signs (of Allah ‘ s sovereignty) for people who have sense .	Al-Baqarah : 2 : 164	For an existence, there must be a reason behind it. Malware program and various Trojan existences made user use her brain to think how to protect her computer for the security purpose. There is always a way to overcome the computer security if user uses her skills and brain to think.
قَالَ بَل رَّبُّكُمْ رَبُّ السَّمَاوَاتِ وَالْأَرْضِ الَّذِي فَطَرَهُنَّ وَأَنَا عَلَى ذَلِكُم مِّنَ الشَّاهِدِينَ	He said : Nay , but your Lord is the Lord of the heavens and the earth , Who created them ; and I am of those who testify unto that .	Al-Anbiyaa : 21 : 56	The virus and the antivirus, the malicious program and computer security system, they all are have been created by human. So, there must be a way to overcome any threat to the computer.

لِيَمِيزَ اللَّهُ الْخَبِيثَ مِنَ الطَّيِّبِ وَيَجْعَلَ الْخَبِيثَ بَعْضَهُ عَلَىٰ بَعْضٍ فَيَرْكُمَهُ جَمِيعاً فَيَجْعَلَهُ فِي جَهَنَّمَ أُولَٰئِكَ هُمُ الْخَاسِرُونَ	That Allah may separate the wicked from the good . The wicked will He place piece upon piece , and heap them all together , and consign them unto hell . Such verily are the losers .	Al-Anfal : 8 : 37	The computer security or the antivirus will be scanning thoroughly the computer and will separate the virus and the working program. The virus then will be compile and will be place in quarantined place or will be removed completely.

Currently Trojan horse attacks, is considered as one of the most serious threats in cyber-attacks. There are many definitions related with Trojan horse such as by (Al-Saadoon& Al-Bayatti, 2011; Saudi, 2008). For this research, Trojan horse is defined as a program that appears as a useful and harmless, and once it has been installed in a victim computer, it begins to carry out malicious acts such as stealing important information from victim's computer. Apart from that, the victim's computer can be controlled remotely.

Though the Trojan horse study was started by Thimbleby and his colleagues (Thimbleby *et al*., 1998), only after 10 years later, more studies were carried out such as by (Chakraborty *et al*., 2009; Karri *et al*., 2010; Tehtanipoor & KouShanfar, 2010; Karri *et al*. & Rosenfeld, 2011). However, these work more focusing on Trojan horse hardware taxonomy and hardware detection techniques instead. Each of these works has it owns strengths and gaps that can be further improved. Zhang *et al.* used timestamp-based data stream clustering algorithm to detect Trojan horse theft activity (Zhang *et al.,* 2012). The researchers used clusters to compress Trojan horse communication data stream information and extracted clusters characteristics for the detection processes. Based on the experiment conducted, it produced 90% an accuracy rate and lower false negative rate. However this work is only focusing on Trojan horse with theft capability.

Apart from that, Tang presented a new Trojan horse detecting method, based on Portable Executable (PE) file static attributes (Tang, 2009). An intelligent information processing technique is used to analyze those static attributes in the PE files. The experiment result showed the test pass rate is 63.90%. The result can be further improved if the experiment involves bigger volume of dataset.

While Liu and his colleagues, used data mining to detect the Trojan horse in Windows environment (Liu *et al.,* 2010). This study shows that the accuracy of classification can be increased when the more relevant features are used in the data mining processes and reduces the consumption of time space. However, the more features are selected, the more time building classification cost, it responds slower in real time and it needs bigger dataset from real network environment. As for work by Dai and his colleagues, they presented a novel malicious code detection approach by mining dynamic instruction sequences (Dai *et al.*, 2009). Their result showed that their approach is accurate, reliable and efficient. But they used dynamic analyses only and when conducting their experiments, the method was not able to detect any malicious code hooked in the remaining part of the executable code. Improvement can be done if their experiment combining both static and dynamic analysis.

Based on all the previous works discussed above, the main challenges whichshould be considered thoroughly are the dataset types and volume, analysis and detection techniques and feature selection to detect the trojan horse efficiently. Therefore, in this research, a new trojan classification is developed by integrating static and dynamicanalyses and by using bigger and standard dataset,which is further explained in Section 3 and Section 4.

METHODOLOGY

In order to produce a new Trojan horse classification, the researchers' had conducted few experiments and researches. A controlled laboratory environment is created to conduct the experiment.The laboratory for this experiment as illustrated in Fig. 2 and Fig. 3. It is a controlled laboratory environment and almost 80% of the software used in this testing is an open source or available on a free basis. No outgoing network connection is allowed for this architecture.

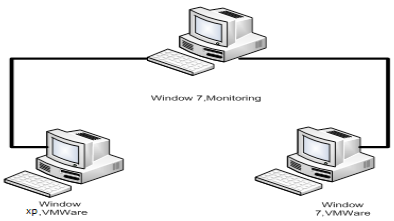

Fig.2.ETCcontrolled laboratory architecture

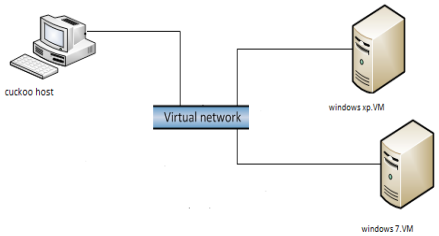

Fig.3. Cuckoo sandbox architecture

Loading specimen: Before loading the specimen into the laboratory, the entire checklist for the analysis must be checked thoroughly. Once the preparation was done, the Trojan horse datasets were loaded into the testing computer using USB memory device. In this lab, the datasets from VXHeavens were tested and analyzed. There are several reasons why this study chose to gather datasets from the VXHeavens source. Firstly, many studies have used this data for their testing. For examples those conducted by (Saudi, 2011), (Dai *et al*., 2009; Schultz and Shumway, 2001; Henchiri & Japkowicz, 2006; Moskovitch *et al*, 2008; Khan *et al*., 2010). The second reason is because the variants are more important than the quantity of the datasets, since this has already represents different types of Trojan horse in VX Heavens and the third is due to the scope of this research, which only focuses on Windows platform. Lastly, it is one of largest Trojan databases freely available from the Internet. A total amount of 1640 Trojan horse datasets have been tested in this lab.

Trojan horse analysis process: The analysis techniques can be divided into two techniques, which are the static and dynamic analyses. To determine the capabilities of these Trojan horses, these two techniques were used in this research lab. The automated analysis, which is part of the dynamic analysis, was conducted using the cuckoo open source software (Cuckoo, 2012). The architecture of the cuckoo can be referred in Fig. 3.All analysis of the Trojan horse, were documented and recorded properly. This record is useful in understanding on how the Trojan horse works. The detailed of the static and dynamic analyses, as the follows:

Static Analysis

The mechanism of the static analysis is by looking at the files associated with the Trojan horse in the computer without running the program.

Anti-virus check: Once the dataset has been loaded into the testing computers, the file type or compression type is identified. Then, the anti-virus that has been installed inside the testing computers is run. It is used to check if the

anti-virus installed can detect anything. If the anti-virus detected the Trojan horse, the name of the Trojan horse is checked and searched in the anti-virus website for further information.

String analysis: String tool called Strings.exe (from Sys internal) is used to extract strings from the Trojan horse codes. This is helpful in identifying the Trojan horse characteristics based on the information retrieved from the strings. Examples of the strings found during the analysis are: Trojan horse specimen's name, user dialog, password for backdoors, URLs associated with the codes, email address of the attacker, help or command-line options, libraries, function calls and other executable used by the Trojan horse.

Looking for script: Based on the strings extracted from the Trojan horse codes, the common scripting or programming languages have been identified as displayed in Table 2.

Disassemble code: Disassemble and debugger which are called as OllyDbg and Ida Pro ,were used to transfer a raw binary executable into assembly language and to disassemble and debug the codes for further analysis.

Scripting Language	Identifying Characteristic Inside the File	File's Common Suffix
Bourne Shell Scripting Language	Starts with the line !#/bin/sh	.sh
Perl	Starts with the line !#/usr/bin/perl	.pl, .perl
JavaScript	Includes the word javascript or JavaScript, especially in the form <Script language = "JavaScript">	.js, .html, .htm
Visual Basic Script (VBScript)	Includes the word VBScript, or the characters vb scattered throughout the file	.vbs, .html,

C++	Can be standalone program or many files referenced within the language	.htm
Active Server Page(ASP)	Can be built using Visual Basic, Jscript or Perl. Can combine HTML, scripts, Active-X server components.	.cpp, .asp

Table 2. IdentifiedCommon Scripting Languages

Dynamic Analysis

Dynamic analysis includes executing the Trojan horse and observing its actions. The Trojan horse is activated in a controlled laboratory environment.

Monitoring file activities: Most Trojan horse reads from or writes to the file system. It might try to write files, altering existed programs, adding new files or append itself to the file system. By using tool such as Filemon, all actions associated with opening, reading, writing, closing and deleting files can be monitored.

Monitoring process: Preview v3.7.3.1 is a tool that is used to monitor any running program, files, registry keys and all of the DLLs in the victim's computer. For each running processes, this tool displayed its owner, personal permission, priority and its environment variables.

Monitoring network activities and registry access: Wire shark is used to sniff the network traffic and Nessus is used to monitor the listening ports. Promiscdetect.exe tool is used to determine if the victim computer in broadcast mode state of the interface. The registry needs to be monitored as it contains all the configuration of the operating system and programs installed in the computer. The registry access is monitored by using the Regmon.

Automatic analysis (malware sandbox): Sandbox is a mechanism to analyze the untrusted files or program in a system. It uses dynamical analysis approach and as an alternative of statically analyze for the binary file. It is an open source, an automated malware analysis system. The sandbox automatically run and analyze files and produces analysis results that outline what the malware does while running inside an isolated Windows operating system. The result report displays the traces of win32 API calls performed by all

processes spawned by the malware, files created, deleted and downloaded by the malware during its execution, memory dumps of the malware processes, network traffic trace in PCAP format, screenshots of Windows desktop taken during the execution of the malware and full memory dumps of the testing computer.

Referring to Fig. 3, this isolated and virtual architecture consists of a host which is installed with Linux (Ubuntu). It is used for guest and analysis management, analyzing, capturing dump traffic and generating reports. While another two virtual computers were setup as a guest and installed with Windows XP Professional and Windows 7 Professional. These 2 computers were used to run and analyze Trojan horse files. Later, the analysis report is sent to cuckoo host to be analyzed.

FINDINGS

This section presents the finding results of the machine learning algorithm. The dataset has been classified using the WEKA (an open source software). Sequential Minimal Optimization (SMO) algorithm is chosen to classify the dataset and the result as displays in Table II. Based on the experiment conducted, SMO algorithm has a better True Positive Rate (TPR) with 98.2% but higher False Positive Rate (FPR) of 1.7%. A comparison with similar work but with different malware classification by Saudi (2011) is carried out. This work used the same source of the dataset. True positive rate (TPR) and false positive rate (FPR) are used during the experiment. The experiment was conducted using the WEKA software.

Table 1.Machine Learning Algorithm Results

Classifier	ETD Mo Results (%)		Comparison work (%)	
	TPR	FPR	TPR	FPR
SMO	98.2	1.7	98.1	0.2

**TPR represents True Positive Rate, FPR represents False Positive Rate.*

The above findings show that an effective way of detecting Trojan has been achieved. With the understanding and applying the meaning of the surah Al-Anfal, verse 53 into cyber security perspective, this Trojan detection method to differentiate between malicious file and normal file has been successfully developed. The following in Table 1, summarized how this Quranic verse has been mapped in this research findings.

Table 2 . Mapping Quranic Verse with Trojan Horse Detection

Quranic Verse	Translation	Mapping to this research paper
	Two seas	The mixture of normal file and malicious file.
	Fresh and sweet	Represents as the normal file.
	Salty and bitter	Represents as malicious file (Trojan horse infected file).
	Barrier	Method to differentiate between malicious file (Trojan horse infected file) and normal file. In this research paper, Sequential Minimal Optimization (SMO) algorithm is chosen to classify the dataset. Based on the experiment conducted, SMO algorithm has a better True Positive Rate (TPR) with 98.2% but higher False Positive Rate (FPR) of 1.7%.

CONCLUSIONS AND FUTURE WORKS

As a conclusion, this research has managed to provide a better TPR which is 98.2%, that outperformed the existing work, where the work has been inspired by surah Al-Anfal, verse 53 (25:53). This result can be used as a reference and comparison by other researchers with the same interests. For future work, different machine learning algorithms will be tested to the dataset produced from this research. This paper is part of a larger project to build up an automated malware clean up model. Ongoing research will include other malware classification and the development of software to automate the malware dataset cleanup.

ACKNOWLEDGMENTS

The authors would like to express their gratitude to Universiti Sains Islam Malaysia (USIM) and Institute Science Islam (ISI),USIM for the support and facilities provided. This research paper is supported by Universiti Sains Islam Malaysia (USIM) grants [PPP/FST/SKTS/30/12712] and [PPP/UCG-0114/FQS/30/11714].

REFERENCES

Al-Saadoon, G, Al-Bayatti, H, 2011. A Comparison of Trojan horse Virus Behavior in Linux and Windows Operating Systems, World of Computer Science and Information Technology Journal,Vol. (1), No. 3, 56-62.

Babak, R., Maslin, B., and Suhaimi, I. (2011). Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey. *International Journal of Computer Science Issues*,*8* (1).

Chakraborty, R.S., Narasimhan, S. and Bhunia, S. 2009. Hardware trojan horse : threats and emerging solutions,Proceedings IEEE International High Level Design Validation and Test Workshop, San Francisco, CA, 166 - 171.

Cuckoo Sandbox Organization, (2012), Cuckoo sandbox, URL: http://docs.cuckoosandbox.org/en/latest/installation/guest/requirements/, [last accessed: 29/1/2015]

Dai,J.,Guha,R.and Lee,J. 2009.Efficient Virus Detection Using Dynamic Instruction Sequences. *JournalofComputers.*Vol4,No5,405-414.

Henchiri, O.and Japkowicz, N.(2006).A Feature Selection and Evaluation Scheme for Computer Virus Detection. *Proceedings of the Sixth International Conference on Data Mining, 2006. ICDM'06.* Hong Kong: IEEEXplore,pp.891.

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

Karbalaie, F., Sami, A and Ahmadi, M**.** (2012).Semantic Malware Detection by Deploying Graph Mining. *International Journal of Computer Science Issues*,*9*(1).

Karri, R., Rajendran,J. and Rosenfeld,K. 2011. Trojan horse taxonomy, In: M. Tehranipoor and C. Wang(eds.), Introduction to Hardware and Security Trust,Springer, pp.325-338.

Karri, R., Rajendran,J.,Rosenfeld,K. and Tehranipoor,M. 2010. Trustworhty hardware: identifying and classifying hardware trojan horse s.Computer 43(10),39-46.

Liu,Y., Zhang,l. Liang,j. Qu,s. Ni,z. 2010.Detecting Trojan horses based on system behavior using machine learning method, 2010 Machine Learning and Cybernetics conference IEEE, vol (2): 855 – 860.

McGraw,K.Hill,G. 2000.Differential effects of end parasitism on the expression of carotenoid-and melanin-based ornamental coloration, Proceedings of the Royal Society of London, Vol (267), 1525-1531.

Moskovitch,R.,Stopel,D.,Feher,C.,Nissim,N.,Japkowicz,N. and Elovici,Y. (2008). Unknown molded detection and the imbalance problem. *Journal In Computer Virology.*Volume5,Number4,295-308,DOI:10.1007/s11416-009-0122-8.

Nguyen, V. T., Kha, V. V., and Anh, A. P. (2012). Research Some Algorithm in Machine Learning and Artificial Immune System, Apply to Set Up A Virus Detection System .*International Journal of Computer Science Issues*, *9*(4).

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

Saudi,M.M (2008). User awareness on virus in windows platform, Journal of Information Technology and Multimedia, UKM.

Schultz ,E.E. and Shumway, Russell.(2001).*Incident Response: A Strategic Guide to Handling System and Network Security Breaches*, 1stedn.,United States of America: New Riders Publishing.

Tehranipoor, M. and Koushanfar, F. 2010. A survey of hardware trojan horse taxonomy and detection, Design & Test of Computers IEEE,Vol(27):1, 10-25.

Thimbleby,H., Anderson,S. and Cairns, P. 1998. A framework for Modelling Trojan horse s and Computer Virus Infection, Computer Journal,Vol(41):7,444-458.

Tang, Sh. 2009. The detection of Trojan horse based on the data mining, Fuzzy Systems and Knowledge Discovery International Conference IEEE, vol (1): 311-314.

Zhang, Xi. Liu, Sh. Meng, L. Shi, Y. 2012. Trojan horse Detection Based on Network Flow Clustering, Multimedia Information Networking and Security conference IEEE: 947-950.

Australia Computer Emergency Response Team (AusCERT), (2013), AusCERT Incident Metrics June 2013, URL:https://www.auscert.org.au/render.html?it=17856