STAKCERT Framework in Eradicating Worms Attack

Madihah Mohd Saudi[1,2], Andrea J Cullen[1], Mike E Woodward[1]
[1]*School of Computing, Informatics and Media, University of Bradford, Bradford, BD7 1DP, United Kingdom*
{M.B.MohdSaudi,A.J.Cullen,M.E.Woodward}@ bradford.ac.uk[1],madihah@usim.edu.my[2]

Abstract

A worm attack is one of the most eye-catching and challenging issues in the cyber world. New and different types of worm attacks are being introduced day by day. Different names have been given to these worms as they evolve such as the 'superworm' and researchers all over the world are trying to find the best remedy to counter such attacks. Loss of money, productivity and reputation are amongst some of the well know implication from these types of attacks. Motivated by the consequences caused by the worm attacks, a new framework called STAKCERT is being proposed. STAKCERT stands for Starter Kit Computer Emergency Response Team. This framework is a novel framework for effective detection, analysis and worm isolation inspired by apoptosis. Apoptosis is also known as cell programmed death; borrowed from the biology term. The STAKCERT framework consists of two stages. The first stage involves the detection and analysis of the worm attack, followed by isolation as the second stage. The uniqueness of this framework is based on the integration of worm, incident response and apoptosis.

1. Introduction

Security has been seen as one of the important elements that should be taken into consideration when dealing with any computer issue such as software, hardware, access control and networks. There are many different techniques, tools and methods that have been applied in the computer security field especially when dealing with the worms attack. But how effective are these approaches? Worm attacks have a big implication especially in terms of the confidentiality, integrity and availability of data. These 3 elements are the most important principles that should be applied in any security environment [1]. If an organization being attacked by a worm for example the W32.Mydoom.A@mm, this worm compromises the confidentiality, availability and integrity of data by sending an email from the infected machine to the names it found in an email address book and ultimately embedding itself via the backdoor of the infected machine. Then, it launches Denial of Service (DoS) attacks on a certain date from the infected machine [2]. This example of a security incident has become worst over the past few years. Indeed, the 'superworm' produced nowadays is the combination of the automated and fast exploitation of vulnerabilities and social engineering techniques [3].

Statistics taken from CyberSecurity [4] show that 3 major security incidents are often reported (i.e. fraud, intrusion and malicious code) as displayed in Figure 1.

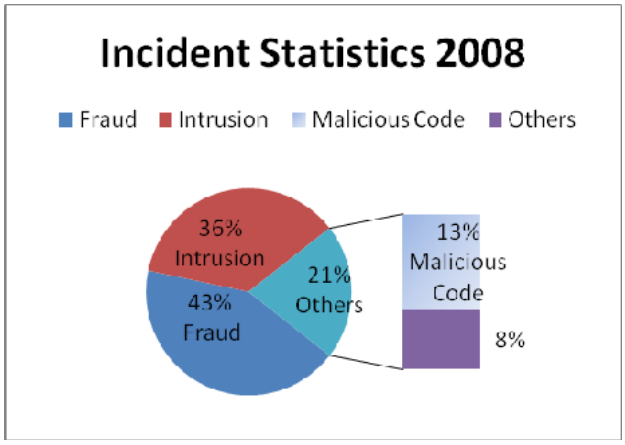

Figure 1. Incident statistics 2008 in Malaysia. Adapted from CyberSecurity Malaysia incident statistics 2008

Indeed, based on the report by Computer Crime & Security (CSI) Survey 2008, [5] one of the most costly computer security incidents was as a result of virus attacks which contributed 49%, of all attacks on organisations that year. If we made a comparison between current trends and those of 10 years ago, these historical attacks were based on the credibility of the attacker and their ability to gain a reputation and

978-0-7695-3791-7/09 $26.00 © 2009 IEEE
DOI 10.1109/CW.2009.13

respect from other attackers or hackers . In contrast the motivation of cyber attacks within the past 5 years, is based on financial gain. Currently attackers try to steal passwords or credit card information through phishing, installed keyloggers and backdoors on end user machines or are involved with launching bots from end user machines to perform ongoing attacks. These cyber attacks have caused insurmountable trouble for many organizations and end users. Indeed, there are still many people that lack the experience or knowledge to detect when their machines are infected by worms [6].

An interesting field that is being integrated in this research is known as apoptosis. Apoptosis, which is also known as programmed cell death, is defined as the capability to kill itself once it has killed the intruder. It is being explored and integrated within this research. It is a natural mechanism where the cells would kill itself when it has become defective and not fulfilled its main function [7].

A framework known as the STAKCERT framework has been developed to determine how worm incidents can be controlled and isolated easily by integrating incident response and apoptosis concepts. STAKCERT stands for Starter Kit Computer Emergency Response Team. Based on this framework, a system called the STAKCERT system will be built.

This research paper consists of the following: Section 2 contains a discussion on previous work; Section 3 and Section 4 explain the project objectives and scope accordingly. Section 5 discusses in-depth the methodology used to build the framework; Section 6 describes the framework design, followed by Section 7 which includes the testing. Section 8 discusses the future work and concludes the paper.

2. Previous works

The need to develop a protective technology to combat worm attacks is seen as one of the challenges in computer worm research. In 1998, White [8] discussed open problems in computer virus research areas which are: heuristic techniques; epidemiology of the virus; the digital immune system; technology in dealing with worms; and proactive approaches to controlling worms. Much research has been carried out since then to answer the problems and challenges raised. In 2006 a paper written by [9] also discussed the open problems in computer virology claiming that until this time, there were only a limited number of studies dealing with computer virology. One field largely ignored that needed to be explored in-depth is the incident response aspect. Incident response is defined as the process that aims to minimize the damage from security incidents and malfunctions and monitors and learns from such incident [10]. It is very hard to separate the incident response field from computer security as it is plays a very important role within this area. Improvements and novel standard operating procedures specifically in detection, analysis and disinfection phases are seen as an area for potential research and exploration.

According to Nazario [11], a worm is defined as an independent replicate and autonomous agent that is capable of searching for new host systems and may infect them through the network. Nazario [11]also divided the worm structure into 6 main components which are: reconnaissance capabilities; special attack capabilities; a command interface; communication capabilities; intelligence capabilities; and unused attack capabilities. They claimed that a worm's divided structure eases the process of worm detection and prevention. Meanwhile Helenius [12] defined a computer worm as an independent program that can replicate recursively by itself. He classified malicious code based on its characteristics and infected objects. Another worm definition is by Skoudis et al [13] where they defined a worm as a self-replicating piece of code which spreads through networks and does not need help from human interaction to propagate. For this research, a worm is defined as malicious software which can replicate itself and move from one computer to another computer or propagate via a network without human intervention or an owner's consent. It can be further classified into a host or a network worm. The worm structure is classified based on the infection mechanism, activation, payload, operating algorithms and propagation mode. This is as illustrated in Figure 5.

Work conducted by [14] made a comparison with the research by [15] using the same data set but with a different approach. This research by [14] has proven to increase the accuracy of a virus classifier using the N-gram method to 93.65% compared to the approach used by [15] which only performs at 63.52% when tested under [14] evaluation method. An improvement can be made to this research by using a retrospective data set which is the combination of old and new worm samples which was applied in the STAKCERT framework. In [14], they focused instead on the old worm sample dataset.

In the incident response field, research conducted by [16] proposed a generic incident response process within a corporate environment. However, research into a combination of worm handling procedures following incidence response is so far scant. It is suggested here that this could greatly improve by detailing the procedure in handling a worm incident. A standard operating procedure of worm incident handling can improve the eradicating time by 90%

from the traditional way by using the STAKCERT's framework.

Apoptosis provides lots of room for exploration to be implemented or integrated into the computer security field. As research by [17] has already discussed regarding the opportunity for integration of the apoptosis concept in distributed mobile services. Security issues such as how to secure the apoptosis are also discussed in this paper. Research by [17] can be used as the basis to form other security tools. The area surrounding the apoptosis concept seems to be largely under researched in the past. However, in the last two years, this is starting to change. In 2007, the HADES system was built by [18], where one of the methodologies used in the system was the programmed death concept. In this system, agents were primarily used for the communication and repair following worm infection, regeneration, movement and death (programmed death). This system is totally reliable on the agents in the system however, flaws might happened due to irregular agent mutation. From a security perspective, a paper by [19] explained how apoptosis can be integrated into computer security.

Based on the previous works discussed in this section, the researchers have conducted an in-depth study and exploration into worm detection and analysis, incident response and apoptosis and have made a correlation between these different fields. This has resulted in the development of a framework, known as the STAKCERT framework.

3. Objectives

The objectives of this research are:

a) To conduct an in-depth study of worm detection techniques and to improve existing techniques in worm detection at host level.(Phase 1)

This is done by developing the existing models in worm detection and by refining specific detectors for worms. The more specific the detector is, the finer its ability is to distinguish between worms that are structurally close to each other. The targeted refined scope will be based on the worm payload. Research carried out by [20] has shown the challenges for future work in confronting worms based on the worm payload itself. Indeed, research by [21] has made a worm classification and one of the categorization was based on payload. This will be developed further here for worm classification and then compared with current research. Later, the worm classification is used to carry out worm detection.

b) To isolate worm infection at host level based on using the apoptosis technique.(Phase 2)

Once the spread of the worm is detected, the step to eliminate any viruses is carried out by integrating the apoptosis technique. A recent study by [19] shows one of the ways to handle viruses is by using the apoptosis concept. The similarities between apoptosis and networks are clearly explained in this paper. Furthermore, this paper also explains on extrinsic and intrinsic apoptosis. In summary, the concept in apoptosis is the same, where it tends to kill itself whenever it discovers that its own self can cause any danger to other attributes around it. Further research on the implementation of apoptosis in distributed services has been carried out by [17]. Their study indicates the potential of exploration of the apoptosis concept.

As from a host level perspective, the proposed elimination technique in this research is such that the host "kills" itself when it finds that it has been infected. This is done by isolating itself, by disallowing services, shutting down server-based applications and locking all unrelated ports. By using this approach, the infected computer will not spread the worm in a network.

c) To produce a STAKCERT framework for handling worm incidents.

The STAKCERT system will be developed based on the STAKCERT's framework in this paper. This system is built to educate end users on computer worms. Following infection, this system helps end users in detecting, analyzing and isolating their system from further propagating the infected worm. This system is built based on expected outcome from objective 1 and objective 2 of this research. The idea proposed by [22] for a security model that focused on 2 layer defense from distributed attacks based on the human immune response system and epidemiology was exciting, however, we also need a pragmatic approach to assist the end user in dealing with the identified problem.

Based on a survey conducted by AUSCERT [23], 14% of the respondents from this survey took no action for their infected machine. Furthermore, this survey also stated that from 70% of the users who updated their anti-virus database, 20% of them still got infected by the malware. Indeed a research study by Panda Labs [24], showed that out of 37.45% of the tested systems in which anti-virus software was up to date, 22.97% still got infected by the malware. There are a few questions as to why these end users still got infected. It might be due to a delay in delivering the update of the anti-virus database or the user simply denies the automated process to clean up the infection. It is clearly seen that sometimes even up to date anti-virus still can miss the new release of the worm. Therefore, a good approach is needed to ensure the end point connect surrounding us is trustworthy and the confidentiality, integrity and availability of the end

point is not questionable and remains free from any worm infection.

From an incident response perspective, the STAKCERT system is build based on standard operating procedures of worm analysis using the Malaysian CERT (MyCERT) procedure [25] (refer to Figure 2). Using this as the basis, a narrow and more detailed standard operating procedure in worm analysis is produced. The research conducted here builds on the earlier work by [25] by developing the incident response aspect of worm infections. The details of STAKCERT system will now be discussed in this paper.

4. Scope

The STAKCERT framework is produced for the use of the end user after the machine has been infected and before the response time. Response time in this research is defined as the help given to the end user before the person in charge to do the eradication comes in (such as the IT personnel, CERT team and anti-virus provider). It is built for windows end points.

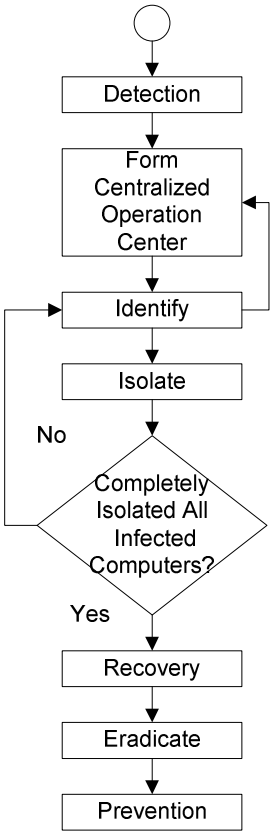

Figure 2. MYyCERT worm IH SOP
Adapted from MyCERT MA-041.052002: computer worm incident handling standard operating procedure 2002

5. Methodology

5.1 Process model of system development: V-Shaped model

This research is conducted as quantitative research. The V-Shaped model has been used as the process model of the system development. It requires the researcher to define the processes involved in system development in detail and incorporates testing during all stages of development. Earlier review and evaluation of requirements in each stage helps to develop any additional requirements and to maintain the quality to generate a quality product.

5.2 Data set and algorithm used

The data set in this research consists of different types of malware. A novel approach has been used in this research where the procedures in worm detection, classification and analysis are well defined by integrating an incident response approach. This dataset has been used as the basis testing the model. To ensure the robustness and accuracy of the system built, the dataset has been expanded. A retrospective approach has been used for the dataset, where it is the combination of datasets from VxHeaven[26] and Offensive Computing[27]. From 66711 samples from the VxHeaven, 5614 were identified as worms. From this figure, 575 which represented 0.86% were identified as the host worm which is the scope for this research. Details of the worm categorization are displayed in Figure 3. From Figure 3, 3.97% represent the Email Worm, followed by 1.36% for P2P worm, 0.96% represents IRC Worm, 0.81% for Internet Worm and 0.42% for Instant Messaging Worm. From the 575 dataset of the host worm, only 504 represented the Windows Host Worm. There were 163 variants of worms from the 504 dataset. The host worm would infect a machine and remains inside the machine and uses the network connection to spread itself to another machines. But it will kill itself after it has replicated itself to other machines [28].

The methodology used here includes the static analysis and dynamic analysis in a controlled lab environment and data mining algorithm known as the Decision Tree (using WEKA software) and Case Based Reasoning for the STAKCERT Framework phase 1. In phase 2, the apoptosis and isolationism algorithm have been integrated. A detailed flow of the framework is explained within the System Design section.

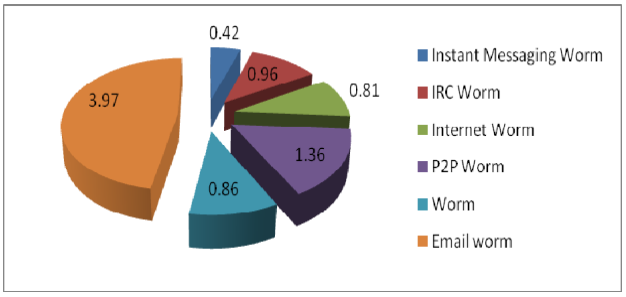

Figure 3. Host worm dataset

5.3 System testing

For system testing, the researchers used a test bed in a controlled lab network as a method to test the framework proposed and the system built. The lab architecture is as displayed in Figure 4. In this lab, the datasets described above were tested. From this testing, the results can easily be measured and any flaws found can be fixed immediately and thus help to improve the quality of the framework and the system.

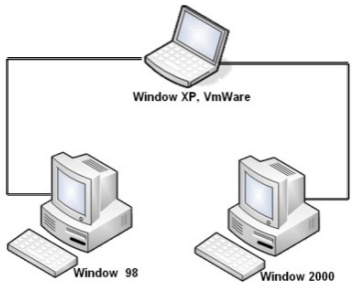

Figure 4. STAKCERT Testing Lab Architecture.

6. Framework design

The following section explains in detail about STAKCERT framework.

6.1 STAKCERT worm classification

This STAKCERT worm classification is produced based on the evaluation and comparison with research by [20] and [21]. The payload has been used as the unique key in identifying the worm for the case study in section 8. The detection and analysis procedures can be developed thoroughly when the worm's structure system being classified based on the STAKCERT worm classification as displayed in Figure 5.

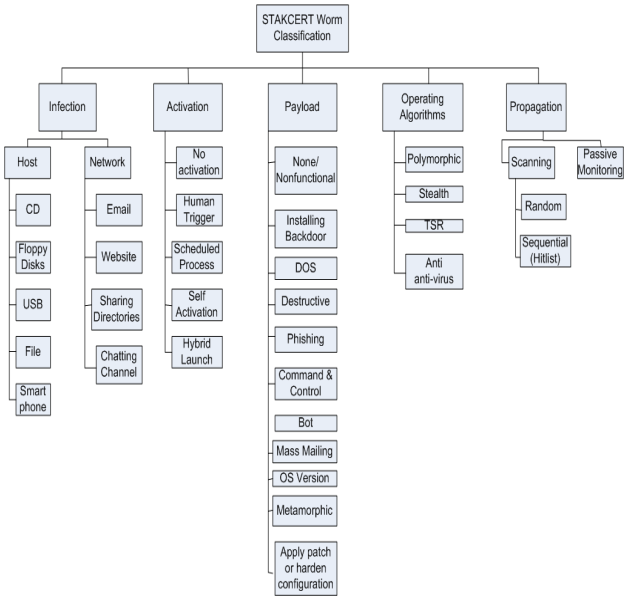

Figure 5.STAKCERT worm classification.

6.2 STAKCERT framework

The STAKCERT system is build based on the framework proposed. The STAKCERT framework involves 2 stages. In the first stage as illustrated in Figure 6, there are 4 main processes which are worm detection, worm analysis, STAKCERT worm classification and data matching.

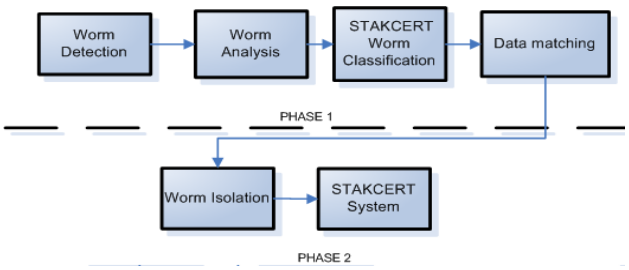

Figure 6. General overview of the STAKCERT framework.

In Phase 2, there are 2 main processes involved which are worm isolation and the formation of STAKCERT system. Under the worm isolation process, a standardize apoptosis technique and isolationism are integrated to control the infected machine from propagating the worms to other machines in the same network.

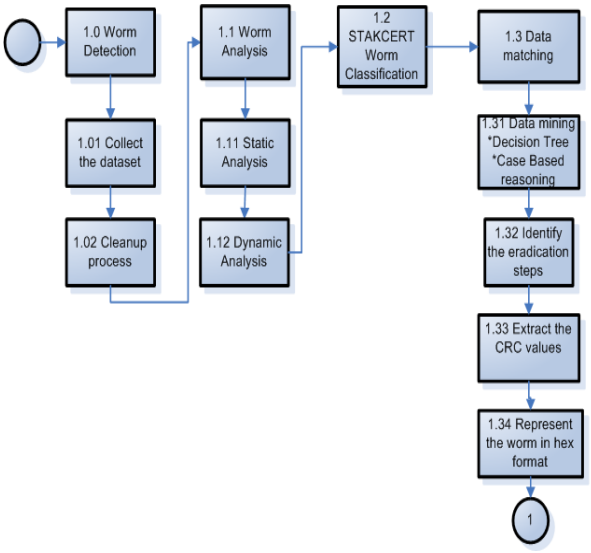

Figure 7. Phase 1 STAKCERT framework.

In Figure 7, the details of Phase 1 of the framework are displayed. Under worm detection, there are 2 processes involved which are the collection of the dataset and the cleanup process. Once completed, worm analysis will take place. This involves static and dynamic analysis. Once the worm has been analyzed, it will be matched with the characteristics in the STAKCERT worm classification. Details of the STAKCERT worm classification are as illustrated in Figure 5. The data matching processes become easier and faster as the result from the processes involved in earlier stages become available. Later the output from Phase 1 is used as the input for Phase 2 in the STAKCERT framework.

7. Testing

A case study was conducted using a sample from VXhaven [17] with the same architecture showed in Figure 4, which was conducted in a controlled lab environment. A static analysis and dynamic analysis had been carried out and the characteristic of the worm were categorized based on the STAKCERT worm classification.

For this case study, the main aims were to test the effectiveness of the framework in stages. Backdoor.IRC.Zcrew, W32.Welchia.Worm, W32.Assarm@mm and W32/Jeefo were used as the sample set to test the framework for phase 1. When anti-virus was used to validate these samples, it was surprising to discover, the Backdoor.IRC.Zcrew had dropped 1 file with a similar name to the genuine window exe file and 2 other files with added names at the front and the back. While for the other 3 sample files, svchost.exe was dropped as one of their payload. The result of the analysis is summarized in Table 1. Please note that all testing was based on the procedures in Figure 7.

Anti-virus Result:

C:\XXX\XXX\XXX\XXX\Backdoor.IRC.Zcrew:\Winmgnt.exe; "Trojan horse BackDoor.Servu";"Infected"

C:\XXX\XXX\XXX\XXX\Backdoor.IRC.Zcrew:\SecureNetbios.exe; "Trojan horse BackDoor.Iroffer.A";"Infected"

C:\XXX\XXX\XXX\XX\Backdoor.IRC.Zcrew:\svchost32.exe; "Trojan horse HideWindow";"Infected"

All of these files as stated in Table 1 had been dropped as the payload by Backdoor.IRC.Zcrew. The file dropped by this malicious code which was the svchost32.exe is similar to the Mimail.I worm. When the analysis was carried out on Mimail.I worm, it was concluded that, even though the way the worms propagate themselves might be different from each other, there is always one similarity which can be identified from these worms. In this case, the payload carried out by these 2 different worms was the same. Another analysis that had been carried out was by referring to Table 1. It shows that the W32.Welchia.Worm used the camouflage technique to spread itself. It used the same genuine windows exe file 'svchost.exe' to fool end user.

Furthermore, a comparison based on other features which are the infection type, activation, operating algorithms and propagation also was conducted. In STAKCERT worm classification, one of the ways to identify worm is being categorized based on the payload. In STAKCERT worm Classification (refer to Figure 5), EDOWA Worm Classification [14] was used as the basis with refinement and enhancement to the payload categorization. Furthermore, the data matching process was becoming easier when payload was used as the unique key identification. Decision Trees have been used to help the data matching process. Once the data matching process was completed, the eradication steps were identified for each worm. Once the eradication steps had been identified, the worm features were clustered together with the eradication steps and the CRC values were extracted and then saved in the database in hex format. This completed the processes in Phase 1.

The strong structure of STAKCERT framework makes the worm detection and analysis job easier and more efficient. The most important part is the procedures involved from the 'Worm Detection' process until 'Representation the worm in hex format'.

By following the procedures accordingly, the analysis can be carried out easily and efficiently, with less time and the result produced can be considered to be highly reliable. In computer security especially from incident response's perspective, no single step should be missed out when handling any incident and each must follow the correct procedures. It had been identified that procedure are often the most neglected and forgotten factor by many organizations and end users. Perhaps this novel framework produced can be used as the basis for organizations and end users in eradicating worm incidents.

Table 1. File name and functionality

Genuine	Fake
1. Netbios.exe -a NetBIOS programming sample that implements an echo server and client	1. SecureNetbios.exe - deletes network shared folders.
2. Svchost.exe- integral part of Windows OS which manages 32-bit DLLs and other services	Svchost32.exe –File used by Mimail.I Worm to exploit infected machine. Svchost.exe – File used by W32.Welchia.Worm, W32.Assarm@mm and W32/Jeefo to exploit infected machine.
3. Winmgnt.exe- Windows Management Instrumentation. It is used by system administrators to create Windows management scripts, for example, scripts that handles the user accounts on a server	Winmgnt.exe - a Serv-U FTP server that being drop by Backdoor.Hale. Trojan Horse.

The output of the STAKCERT framework Phase 1 is later used as the input for STAKCERT framework Phase 2. In STAKCERT framework Phase 2, the two main processes involved are worm isolation and STAKCERT system formation. In worm isolation, a few challenges have to be taken into consideration as follows:

a) The threshold value to trigger the isolation process.
b) The implication to the end user machine when the apoptosis takes place.
c) The integrity of the apoptosis activator from being tampered with by other malicious processes.

Once these challenges have been solved, a STAKCERT system can be formed easily. To test the effectiveness and the robustness of Phase 2, a retrospective dataset has been used which is a comination of different datasets to avoid bias in system identification.

8. Conclusion and Future Work

Procedures play a big role in worm detection, classification and analysis. Lack of understanding in incident response procedures might lead to bigger problems in handling worms. The STAKCERT framework proposed in this paper is the outcome of the integration between worm, incident response and the apoptosis field which are blended together to produce an efficient worm incident handling framework. For future work, the scope of this research will be broadened to spyware and botnets. Integration with an agent is seen as a way of improvement for the performance in worm detection, classification and analysis. This paper is part of a larger research project to confront worm attack. Ongoing research includes producing a STAKCERT system based on the STAKCERT's framework. This framework can be used as the basis for further research in the malicious code field.

9. Acknowledgement

The authors would like to express their gratitude to School of Computing, Informatics and Media, University of Bradford and Universiti Sains Islam Malaysia (USIM) for the support and facilities provided.

10. References

[1] Rick Lehtinen, Deborah Russell and G.T. Gangemi Sr, " Computer Security Basics", 2nd Edition, O'Reilly Media, Inc., Sebastopol, CA, 2006, ISBN: 0-596-00669-1, pp. 10-12.

[2] Symantec website, (2007), W32.Mydoom.A@mm, URL: http://www.symantec.com/security_response/writeup.jsp?docid=2004-012612-5422-99 [last accessed: 21/6/2009]

[3] Ivan Balepin, " Superworms and Cryptology: a Deadly Combination", 2003, URL: http://vx.netlux.org/lib/aib01.html , [last accessed: 21/6/2009]

[4] CyberSecurity Malaysia, "Incident Statistics 2008", 2008, URL: http://mycert.org.my/en/services/statistic/mycert/2008/ main/detail/566/index.html [last accessed: 21/6/2009]

[5] Richardson, Robert, *"CSI Computer Crime and Security Survey",* 2008, URL: http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf [last accessed: 21/6/2009]

[6] Schroeder, Chris, “Home Networks, Safe or Sane*?”* , CA: Canaudit,Inc. Volume 6, Issue 3,2005. [last accessed: 21/6/2009]

[7] L. B. Goncharova, Y. Jacques, C. Martin-Vide, A. O. Tarakanov and J. I. Timmis, "Biomolecular Immune-Computer: Theoretical Basis and Experimental Simulator," *Artificial Immune Systems*, Lecture Notes in Computer Science, pp. 72-85: Springer Berlin / Heidelberg, 2005

[8] Steve R. White. “Open problems in computer virus research”. In *Proceedings of theVirus Bulletin Conference*, Oct 1998.

[9] E. Filiol*, M. Helenius and S. Zaner.*, "Open Problems in Computer Virology," *Journal in Computer Virology,* vol. 1, pp. 55-66, 2006-03-11 2006.

[10] BSI. “Information security management, BS7799, part 1: code of practice for information security management”, 1999.

[11] Jose Nazario, Jeremy Anderson, Rick Wash and Chris Conelly, (2001), “ The Future of Internet Worms”, In Proceedings Black Hat Conference, USA. URL: http://www-personal.si.umich.edu/~rwash/pubs/worm.pdf. [last accessed: 21/6/2009]

[12] Marko Helenius (2002), “ A System to Support the analysis of Antivirus Products’ Virus Detection Capabilities”, PhD Thesis, Department of Computer & Information Sciences, University of Tampere. URL: http://acta.uta.fi/pdf/951-44-5394-8.pdf. [last accessed: 21/6/2009]

[13] Ed Skoudis and Lenny Zelster, “ Malware Fighting Malicious Code”, Pearson Education,Inc., New Jersey, 2004.pp.71-88.

[14] Olivier Henchiri, Nathalie Japkowicz, "A Feature Selection and Evaluation Scheme for Computer Virus Detection", *In Proceedings Sixth IEEE International Conference on Data Mining (ICDM'06),* pp.891-895, 2006. [last accessed: 21/6/2009]

[15] Matthew G. Schultz, Eleazar Eskin, Erez Zadok and Salvatore J. Stolfo, “Data Mining Methods for Detection of New Malicious Executables”, *In Proceedings of the 2001 IEEE Symposium on Security and Privacy*, IEEE Computer Society, pp 38, 2001. [last accessed: 21/6/2009]

[16] Mitropoulos, S., Patsos, D. & Douligeris, C. *“On Incident Handling and Response: A state-of-the-art approach”, Computers & Security*, Volume 25, pp.351-370, 2006. [last accessed: 21/6/2009]

[17] C. Tschudin, “Apoptosis — the Programmed Death of Distributed Services”, *Secure Internet Programming, Lecture Notes in Computer Science,* Volume 1603/1999, Springer Berlin / Heidelberg, pp.253-260, 1999.

[18] M.M. Olsen, N. Siegelmann-Danieli and H.T. Siegelmann, “Robust artificial life via artificial programmed death”, *International Journal of Artificial Intelligence,* Volume 172, Issues 6-7, Elsevier B.V, pp. 884-898,2008

[19] Madihah Mohd Saudi, Andrea J Cullen, Mike E Woodward, and Hanina Mohd Noor, “An Overview of Apoptosis for Computer Security”, *Proceedings International Symposium on Information Technology* 2008*(ITSIM’08),* Volume IV, KL ,. pp. 1-6, 27-28 August 2008.

[20] Arshan Dabirsiaghi, “Building and Stopping Next Generation XSS Worms”, *In Proceedings 3rd International OWASP Symposium on Web Application Security Conference Europe 2008*, 2008. [last accessed: 21/6/2009]

[21] Madihah Mohd Saudi, Emran Mohd Tamil, Siti Aishah Md Nor, Mohd Yamani Idna Idris and Kamaruzzaman Seman,"EDOWA Worm Classification", *In Proceedings of the 2008 International Conference of Information Security and Internet Engineering (ICISIE 2008),* 2-4 July 2008 London.

[22] Goel, S. & Gangolly, J. S. “On decision support for distributed systems protection: A perspective based on the human immune response system and epidemiology”, *International Journal of Information Management*, Volume 27, pp.266-278, 2007.

[23]AUSCERT website, “AusCERT Home Users Computer Security Survey 2008”, 2008, URL: http://www.auscert.org.au/images/AusCERT_Home_Users_ Security_Survey_2008.pdf. [last accessed: 21/6/2009]

[24] PandaLabs, “Malware infections in protected systems”, 2007,URL: http://www.pandasecurity.com. [last accessed: 21/6/2009]

[25] MyCERT website, “MA-041.052002: Computer Worm Incident Handling Standard Operating Procedure” ,2002, URL: http://www.mycert.org.my/data/content_files/ 10/49.jpg?diff=1187214823 [last accessed: 21/6/2009]

[26] Vxheaven website, “Virus Collection”, 2009, URL: http://vx.netlux.org/vl.php. [last accessed: 21/6/2009]].

[27] Offensive Computing website (2009), “Malware search”, URL: http://62nds.com/pg/e90.php [last accessed: 21/6/2009]

[28]Nick FitzGerald, “What is a Worm?(Computer Virus)”, URL: http://stason.org/TULARC/security/computer-virus-l/11-What-is-a-Worm-Computer-virus.html. [last accessed: 21/6/2009].