Pan, Jonathan; Fung, Chun Che

Conference Paper

Pattern for Malware remediation: A last dine of defence tool against malware in the global communication platform

19th Biennial Conference of the International Telecommunications Society (ITS): "Moving Forward with Future Technologies: Opening a Platform for All", Bangkok, Thailand, 18th-21th November 2012

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Pan, Jonathan; Fung, Chun Che (2012) : Pattern for Malware remediation: A last dine of defence tool against malware in the global communication platform, 19th Biennial Conference of the International Telecommunications Society (ITS): "Moving Forward with Future Technologies: Opening a Platform for All", Bangkok, Thailand, 18th-21th November 2012, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/72489

ITS 2012 Bangkok
Moving Forward with Future Technologies : OPENING A PLATFORM FOR ALL

Proceedings of the 19th ITS Biennial Conference 2012 Bangkok, Thailand

Pattern For Malware Remediation – A Last Line of Defence Tool against Malware in the Global Communication Platform

By

Jonathan Pan, Chun Che Fung

Pattern For Malware Remediation – A Last Line of Defence Tool against Malware in the Global Communication Platform

Jonathan Pan
School of Information Technology, Murdoch University, Perth, WA, Australia
Jonathan.Pan.JY@gmail.com

Chun Che Fung
School of Information Technology, Murdoch University, Perth, WA, Australia
l.fung@murdoch.edu.au

Abstract

Malware is becoming a major problem to every organization that operates on the global communication platform. The malicious software programs are advancing in sophistication in many ways in order to defeat harden deployed defenses. When an organization's defense fails to keep this malice invasion out, the organization would incur significant amount of risks and damages. Risks include data leakage, inability to operate and tarnished corporate image. Damages include compensation costs to customers and partners, service unavailability and loss of customers' and partners' confidence in the organization. This in turn will affect the organization's business continuity. In order to manage the risks and damages induced by Malware incidents, incident responders are called upon to be the last line of defense against the digital onslaught assault. However incident responders are challenged too by the deep levels of knowledge, skills and experience required to contain the ever advancing and persistent Malware. This paper proposes the establishment of a Pattern template for Malware Remediation to aid incident responders to overcome their competency limitations in order to provide organizations the tool to repel Malware and to reduce the associated risks. Examples and details of the proposed patters are provided with discussions on future direction of the research work.

Keywords – Pattern, Malware Remediation, Global Communication Platform

I. INTRODUCTION

Malware is a significant threat to organizations and individuals. The Organization for Economic Co-operation and Development (OECD) has already acknowledged the risks and threats imposed by Malware in their 2007 report [1]. Besides being a threat, Malware inflicts the consumption of additional resources and cost to fend off this malice. The consumption is still rising [2]. While organizations' expenses are increased to build defenses against this malice, some highly sophisticated Malware are still able to render the defenses ineffective. There are two main reasons to this. First is the ever advancement of Malware's sophistication is causing the defense solution vendors to take a catch up or reactive posture in the battlefront. Secondly, human is the primary cause to the defense solutions inability to keep the malice at bay due to ignorance or omission [25]. Hence, Malware has proven to have the upper hand in its ability to penetrate and defeat these defenses.

The primary effect of a Malware penetration into an organizations' Information Technology (IT) environment is the lost of control over IT assets by the affected organization. The following table illustrates the qualitative impact to an organization that loses control of its IT assets to Malware.

Security Risks	Organization having More Control	Malware having More Control
Confidentiality	Reduces data leakage, protects confidentiality	Increases data leakage, losses confidentiality
Integrity	Improves security posture, improves reliability of IT assets	Degrades security posture, degrades reliability of IT assets

Availability	Improves resiliency, enhances business continuity	Degrades resiliency, affects business continuity

Table 1. Security Risks Of Malware Control To Organizations.

When a Malware takes control of an organization's IT assets, the organization has to respond and remediate the effects and risks induced by the Malware promptly. Such responsive actions may be carried out by formally or ad-hocly established incident response team. Their objective is to restore control of IT assets back to the organization through Malware remediation or containment. However, these incident responders face a number of challenges in their battle to restore control. A key challenge is the deep competency (knowledge, skills and experience) requirements over the incident responders, and their ability to keep pace with the ever-advancing Malware technologies and contemporary weaponry used in the skirmishes between attackers and defenders.

The lack of such competencies will result in delay and having a response plan that is limited or ineffective in remediating the Malware incident. This will in turn induces greater risks to the organizations. Incident responders therefore urgently require assistance to help them to overcome the limitations and to enable them to achieve the objectives to defunct the Malware and restore control of IT assets back to the organizations. This paper will cover the details of this challenge faced by incident responders. This is followed by a survey of the related research work reported previously on addressing this problem. Next, a proposal based on Malware Remediation pattern template is discussed in order to aid incident responders to deal with the abovementioned challenges. This is subsequently followed by two examples of Malware Remediation techniques mapped to the proposed Malware Remediation pattern template. Finally, a conclusion and a list of future research options are given.

II. NEED TO RE-ENFORCE NEW DEFENCE LINE

When a Malware successfully gets past deployed defenses and infects an organization's or individual's computing host(s), Malware Remediation becomes the new line of defense. However the new defense line, manned by incident responders, is under immense pressure with its deep competency requirements in order to match the evasive and complex Malware.

A. Challenges from Malware

The Malware adversary is advancing in its ability to carry out its malicious mission. They can evade detection and persistently remain active as long as intended and they are able to fend off any attempts to eradicate them. Malware developers have incorporated many features to enhance their products' evasive capability. They have embedded stealth capabilities into their products through various forms of obfuscation and abusive use of legitimate services. They have incorporated artificial intelligence [2] to adapt their Malware to the environment in order to camouflage their Malware from being detected and eradicated.

Malware developers are also increasingly incorporating advanced techniques used in software resilience designs. Design techniques like configuration redundancy, active monitoring of the configuration, regular updates to enhance software resiliency and deep entrenchment into the core of the operating system. With such resiliency designs, the Malware is capable of surviving attempts to defunct or eradicate it.

Malware developers are also incorporating abilities to circumvent all forms of deployed defenses like Anti-virus, Firewall and Intrusion Detection or Prevention systems [4]. In addition, these defenses are now becoming victims of Malware self-preservation attacks [5]. Modern Malware can defunct the operational effectiveness of these defenses to remove the intended protection deployed to protect against loss of control over IT assets [6]. Malware developers are also incorporating mechanisms, like disabling specific operating system services or regular product updates, to prevent attempts by incident responders or forensic investigators to conduct containment or analysis [7]. Anti-forensic mechanisms like encryption capabilities are frequently used in the designs of Malware [8].

In recent times, there is an increasing number of Malware that are uniquely developed to target specific individuals and organizations [9]. Such boutique Malware are custom made to stay clear of deployed defenses rendering the latter ineffective.

B. Needs of Incident Responders

Incident responders have a number of challenges to overcome when conducting Malware Remediation. Specifically covered in this paper, the challenge is on acquiring the needed competency. When a Malware successfully infiltrates pass the defenses and starts to induce risks to an organization, the incident responders will first need to understand how the involved Malware works. According to Valli and Brand [10], the body of knowledge in the area of Malware analysis covers a wide area of topics from core IT subjects to forensic analysis, to knowledge in the use of a wide variety of IT tools such as administrative and forensic tools.

When attempting to understand the Malware involved in an incident, incident responders need to identify the identity of the Malware, understand its corresponding behavior and subsequently define the appropriate remediation options. The number of possible Malware suspects to the incident is massive with many new ones being created daily. In McAfee's third quarter's threat report for 2011, it estimates that there will be 75 million Malware by the end 2011 [11]. This poses a significant challenge to incident responders in attempting to identify the Malware involved and its associated remediation options. To further complicate the situation, the analysis of Malware would likely to be done over infected computers and is less likely over the original source malicious file or material. When such information is not readily available, the incident responders will need to dig deeper into system like server logs to sift out useful information. Under such circumstance, the incident responders will need more skills and knowledge in the setup and operations of the IT infrastructure environment in which the Malware is roaming or spreading. Also, Malware is exploiting zero day exploits from a constant stream of unknown vulnerabilities in which, even at the time of incident, the original equipment manufacturer (OEM) of the software or appliance may not be aware of the existence of the vulnerability. Hence the incident responder may be required to isolate the exploit and to deal with the vulnerability in order to mitigate the further risks induced by the Malware.

Experience in performing Malware Remediation will aid in the management of risks associated with such cyber security incidents [12]. Experience in navigating through the IT operating environment and identifying ways to best leverage on the existing deployed security defenses, though they first failed to stop the Malware infiltration, may prove effective still in subsequent containment effort of the Malware. Additionally prior experience in handling Malware will enhance the responders' ability to shorten the duration needed to defunct the Malware involved. While the number of Malware is growing at a rapid rate, most of the new Malware are variants of previous versions of Malware [26]. Hence, prior experience in handling Malware will help the incident responders. Finally, experience will play an important contributor to the relevance and usefulness of certain containment techniques for specific Malware or situational conditions.

When incident responders lack such required competency, they will have difficulty in identifying an effective remediation plan. An ineffective remediation may cause more damage or induced more risks to the organization. There are Malware which can detect remediation attempts and they are able to launch an adverse counter offense against the organization. Malware have known to destroy data that they have control when they sense an attempt to contain them [13]. Additionally, incompetent incident responders may likely to incur significantly more time to remediate the Malware problems. According to Verizon's report, Malware containment or remediation is taking a lot of time [14]. Infection occurs within seconds to minutes while containments last days to months. According to Logan and Logan [15], the remediation of Malware outbreak took 7 days before the computers were safe to be used again. As mentioned earlier, as the Malware gains and keeps control over important IT assets, the risk exposure escalates over time.

What is required of incident responders is the ability to quickly identify a remediation solution that can effectively contain or defunct the Malware involved. However the current situation in the real world looks bleak. In order to address this limitation, it is believed that a form of knowledge repository is required to be established with a comprehensive set of containment / remediation techniques that can be leveraged upon quickly to improve the outcome of remediation plans in terms of effectiveness to defunct the Malware and to reduce the duration in which the remediation plan is identified and applied. Therefore, a structure or format to store and represent such knowledge in a repository is first required.

III. RESEARCH PROPOSITION

The research proposition in this paper is to establish a Malware Remediation pattern template to address the abovementioned problem. This will enable the establishment of a knowledge repository for Malware Remediation that is to be developed in the future but not covered in this paper. Based on current research, it was found that such pattern template does not exist. The proposed Malware Remediation pattern template is based on security pattern template. Before going into the specifics of the proposed pattern template, some background information about pattern is provided below.

A. Patterns – Introduction

Patterns may be defined as solutions to common occurring problems that occur within a specific context. Patterns could encapsulate knowledge and understanding as regard to a particular problem hence they could be used to express knowledge from experienced individuals or group of practitioners. According to May and Taylor [27], patterns can be used to improve the process of converting information to knowledge as part of knowledge management. Patterns may also be used to describe procedures and artefacts produced by processes [16]. Good patterns are like cooking recipes: they inform what elements are required and they provide a sequence of step instructions or approaches on how to use the ingredients and the expected outcomes or products. Patterns could also include important contextual information like when the solutions are applicable and when they are not (also known as anti-patterns), what they will accomplish and how to adapt them to specific situations. They will also state consequential effects when the actions are applied.

Patterns are useful tools for solving multidisciplinary problems. In areas where there is a lack of skills or knowledge, patterns can help address the deficit by pre-packaging solutions to common problems. They enable reuse of successful practices. Patterns could be used to capture the experience from experts in a structured way [17]. Thus novices can benefit from the know-how and skills of people who have put much effort into the understanding of the contexts, forces, and solutions. Patterns have also been used to facilitate teaching by experienced teachers and to aid students' learning. They are known as Pedagogical Patterns [18].

B. Malware Remediation Patterns – Research Proposition

There are many forms of patterns that exist in academia and implementation practices. They include software design patterns that provide a knowledge repository of good software designs approaches. Security pattern is another example. Schumacher and Roedig [17] stated, "A security pattern describes a particular recurring security problem that arises in specific contexts and presents a well-proven generic scheme for its solution." Hence, this proposition for a Malware Remediation pattern template derives from the concept of security pattern template. Details to justify this proposition will be covered in subsequent sections.

IV. RELATED WORK

There is limited information or knowledge repository relating to Malware Remediation. On the other hand, most of the information has focused on Malware detection and security

hardening solutions rather than remediation. The following evaluates the limitedly available information sources and their structure, other related forms of knowledge representation and a relevant pattern template.

A. Remediation Guide

There are a number of guides provided by various organizations and individuals to aid incident responders in dealing with Malware outbreak. An example is the National Institute of Standards and Technology's (NIST) "Guide to Malware Incident Prevention and Handling" [12] and "Computer Security Incident Handling Guide" [19]. Other related computer security agencies or organizations have produced similar materials. Most of these guides proposed various approaches to contain a Malware outbreak. However, these guides lack a unified structure in the way information is organized. In some cases, they lack the important information that is relevant to the incident, and what should have been considered prior to the application of the approaches. For example, considerations to the use of such approaches like prerequisites and consequential effects like the residual risks from the use of the approach are examples of omission. Also, they are short of cited examples to illustrate how the solution can be applied and links to related approaches.

B. Knowledge Management in IT Security

Kesh and Ratnasingam [28] argued that knowledge management is an important tool that an organization can use to protect itself from hackers, Malware, theft of data and service disruption by providing security knowledge to the right people in the organization. They further argued that knowledge management practices should be applied to all stakeholders in the organization who are involved in the security management process. There are various attempts to structure security knowledge. Examples include the use of ontology [29] and patterns. There are attempts to cover different areas of security including software security [30]. However there is no knowledge management template for Malware Remediation.

C. Security Patterns

Saltzer and Schroeder [20] introduced the concept of using design principles to improve the security of computer systems in their classic article, "The Protection of Information in Computer Systems." Inadequate security in IT systems creates opportunities for exploitation. Security exploitation in IT may occur in the form of Malware outbreak induced by software vulnerabilities and weak mechanisms in protocols or software designs that are compromised through exploitation. Schumacher and Roedig [17] advocated that when deficiency exists in security engineering in IT solutions, security patterns can aid in addressing this gap. According to Kienzle et al. [21], "A security pattern is a well-understood solution to a recurring information security problem." They are the concepts advocated by Christopher Alexander they were applied to the domain of information security. While some of such security patterns take the form of design patterns, not all security patterns are design patterns.

Schumacher and Roedig argued that security patterns provide four significant benefits. First, patterns provide guided knowledge in security to non security experts. This is because security patterns capture the know-how and skills of security experts, thus enabling novices to act as security experts. The second benefit is that security professionals can exchange ideas and work on security issues effectively. This is because security patterns encompass both the security problems and solutions. They limit ad-hoc solutions as patterns are defined to represent proven solutions in a systematic and organized manner. The third benefit is that security patterns address security problems in structured approaches. Patterns explicitly cite qualifications and implications if any, so that an informed decision may be made before a particular pattern is applied. Finally, security patterns detail component dependencies and associations to other security patterns or issues. Such knowledge and illustrated examples are typically acquired through experience. When security patterns are linked or formally associated, changes that affect certain security patterns or problems will have impacts to other

linked security patterns. Hence this would induce the need for refactoring of patterns to be done regularly to ensure that the security patterns are relevantly updated in the face of constant change.

According to Heyman et al. [22], security patterns can be applied to many aspects of security from security assessment to security development lifecycle and security audits and recovery. However, there is no security pattern for Malware Remediation. Hence to address the problems faced by Malware incident responders, this paper advocates the establishment of the Malware Remediation pattern template.

V. METHODOLOGY

This research proposition entails the use of security pattern template to represent Malware Remediation pattern template. The reasons for this proposition are firstly that Malware Remediation is a form of IT security incident response to deal with a security risk when there is a Malware outbreak. Hence it relates to security. Secondly, security patterns have been used to many aspects of security including incident response and disaster recovery in which Malware outbreak or infection is a form of disaster that could become catastrophic.

The following details a proposed Malware Remediation pattern template derived from a generic Security Pattern template advocated by Yoshioka et al [23]. The Pedagogical Patterns also uses the similar structure.

- ***Pattern Name***: This is the primary key to the pattern. It should be self-explanatory and intuitive in order to improve communication and to facilitate search.
- ***Problem***: This describes the Malware incident problem that may be solved by the application of the Malware Remediation pattern.
- ***Context***: Describes the context in which the problem exists. It should state the environmental situation in which the pattern can be best used.
- ***Pre-requisite***: This describes the properties that must be fulfilled prior to the start of the implementation of the pattern. It may entail environmental conditions or settings needed to support the pattern.
- ***Solution***: This describes the specific pattern implementation details. It may include various forms of details depending on the context in which the pattern is applied. It may be qualitatively and quantitatively described. For example, for software designs, UML or pseudo codes may be used.
- ***Example***: This provides an illustration or references on how the pattern solution may be or has been applied.
- ***Consequence***: This provides details of likely residual risks or impact from the use of the pattern. This is important to ensure that the pattern user makes an informed decision prior to the use of the pattern and prepares the necessary to handle the consequences.
- ***Related Patterns or References***: This provides references or linkages to materials used to produce this pattern or other patterns may be relevant or used in congruent to this pattern.

These elements are required to provide details on why the pattern is relevant [Problem], where the pattern should apply [Context], when to apply [Pre-requisite], what is the impact after its application [Consequence], and finally how, with details, is the pattern applied [Solution]. The [Examples] and [References] provide relevant associations to other patterns or techniques. The followings are two examples of published techniques for containment by NIST mapped into the proposed Malware Remediation pattern template. Quotes are used when the exact text from the guide are included in the pattern draft.

A. Pattern 1 – Containment through Disabling Services

The following Malware Remediation pattern is drafted using information from NIST's "Guide to Malware Incident Prevention and Handling" that advocated disabling services used by the Malware. The following is a pattern write-up for this.

Pattern Element	Pattern Details
Name	Containment through Disabling Services
Problem	Malware has infiltrated environment and managed to get pass deployed defenses with no detection and containment occurring from the latter.
Context	Malware is exploiting specific network service(s) as part of its infection or attack vector. "*An incident might generate so much network traffic or application activity, such as e-mails or file transfers that many applications could effectively be made unavailable*."
Pre-requisite	a. Able to identify which services that Malware is using for its infection or attack vectors b. Identified service can be disabled as part of remediation. Business continuity plans may be required to mitigate the effects of service outage.
Solution	"*Containing such an incident quickly and effectively might be accomplished through a loss of services, such as shutting down a service used by malware, blocking a certain service at the network perimeter, or disabling portions of a service (e.g., large mailing lists)*". "*Shutting down the affected services might be the best way to contain the infection without losing all services*". Depending on the situation and severity, network service outage in selected subnet instead of the entire network will aid in the remediating the effects of the Malware outbreak. The extent of the service outage is dependent on the characteristics of the Malware involved.
Example	A response guide recommendation by NIST
Con-sequence	"*Disabling a service is generally a simple process; understanding the consequences of doing so tends to be more challenging*" a. Malware may adapt or update its strategy when it detects that its dependent network services are not available. b. Malware may launch countermeasure offensive when it detects service unavailability. c. "*Disabling a service that the organization relies on has an obvious negative impact on the organization's functions. Also, disabling a service might inadvertently disrupt other services that depend on it*" "*Organizations should maintain a list of dependencies between major services so that incident handlers are aware of them when making containment decisions. Also, organizations might find it helpful to provide alternative services with similar functionality*". d. "*Organizations should also be prepared to respond to problems caused by other organizations disabling their own services in response to a malware incident*".
Related Patterns or References	• Guide to Malware Incident Prevention and Handling by NIST (Para. 4.3.4) • Computer Security Incident Handling Guide (Para. 3.3.4)

Table 2. Containment through Disabling Services Pattern.

B. Pattern 2 – Containment through Disabling Connectivity

The following containment pattern is drafted using NIST's "Guide to Malware Incident Prevention and Handling" that advocated disabling connectivity used by the Malware. The following is a pattern write-up for this.

Pattern Element	Pattern Details
Name	Containment through Disabling Connectivity
Problem	Malware has infiltrated environment and managed to get pass deployed defenses with no detection and containment occurring from the latter.
Context	Malware is using connectivity as part of its infection or attack vector. This may pose significant risks especially when the Malware is stealing data and sending data out through the network connectivity into the intended destination.
Pre-requisite	a. Able to identify which the connectivity route that Malware is using b. "*Organizations can design and implement their networks to make containment through loss of connectivity easier to do and less disruptive*."
Solution	"*Containing incidents by placing temporary restrictions on network connectivity". "If infected systems within the organization attempt to spread their malware, the organization might block network traffic from the systems' IP addresses to control the situation while the infected hosts are physically located and disinfected*". "*An alternative to blocking network access for particular IP addresses is to disconnect the infected systems from the network, which could be accomplished by reconfiguring network devices to deny network access or physically disconnecting network cables or ejecting removable network interface cards from infected systems.*" "*The most drastic containment step is purposely breaking needed network connectivity for uninfected systems*". "*In worst-case scenarios, isolating subnets from the primary network or even disconnecting the entire organization from the Internet might be necessary to stop the spread of malware, halt damage to systems, and provide an opportunity to mitigate vulnerabilities*".
Example	A response guide recommendation by NIST
Con-sequence	a. Malware may adapt or update its strategy when it detects that its dependent network connectivity is not available. b. Malware may launch countermeasure offensive when it detects connectivity unavailability. c. Business or IT operations dependent on the connectivity will be affected. Hence contingency plans will need to invoke.
Related Patterns or References	• Guide to Malware Incident Prevention and Handling by NIST (Para. 4.3.4) • Computer Security Incident Handling Guide (Para. 3.3.4)

Table 3. Containment Through Disabling Connectivity Pattern.

VI. ANALYSIS

The mapping exercise from NIST's guide document to our pattern template was seamlessly done as the NIST guide write-up was comprehensive and detailed. It is also shown that the proposed containment pattern template for incident responders is adequate enough to represent such forms of knowledge as the NIST's guide was intended for such a purpose. The benefits that the proposed pattern offered above and beyond what is included in the NIST's guide is the structure that imposes and linkages to other materials to enable fast adoption of knowledge and leverage on documented experience. Detailed steps of the remediation were not included in the NIST's guide hence it was not included in the pattern drafts too. Future iterations of the patterns should include detailed steps to further simplify adoption.

VII. CONCLUSION

Malware Remediation or containment is now recognized as the new line of defense for organizations and individuals who are constantly subjected to persistent onslaught of Malware attacks [61] that in turn affects business continuity of organizations. Incident responders, who are the defenders of this line of defense, are challenged by the ever advancing Malware. This paper addressed the key challenge faced by incident responders, which is the deep competency requirements of knowledge, skills and experience to aid in containing the attacking Malware. To overcome this limitations, incident responders will need a repository of Malware Remediation patterns that will aid them to shorten the learning curve requirements and possibly shorten the Malware Remediation duration. Also, when the repository is timely updated with new threats from Malware, the Malware Remediation competency will remain to be relevant. Our research proposition for a Malware Remediation pattern template is an important step towards establishing such a repository. In order for the pattern template and pattern knowledge repository to stay relevant, they should be maintained and updated by an open community of practitioners from the academia, security industry and security incident response practice.

For future research directions, new containment patterns will be added to the repository. Also, patterns can be formally specified and verified. Patterns can also be coded using forms of ontology to extend this knowledge repository to integrate with other knowledge repositories like Common Vulnerabilities and Exposures (CVE) and Malware Attribute Enumeration and Characterization (MAEC) from Mitre [24]. It is believed that the use of such patterns will be a great help to security Incident Responders.

VIII. REFERENCES

[1] OECD Working Party on Information Security and Privacy (WPISP) in partnership with the Asia Pacific Economic Co-operation Telecommunication and Information Working Group (APEC TEL) Security and Prosperity Steering Group (SPSG), "Malicious Software (Malware): A Security Treat to the Internet Economy", OECD Ministerial Meeting on the Future of the Internet Economy, DSTI/ICCP/REG(2007)5/FINAL, Jun. 17, 2007.

[2] Lumension, "State of Endpoint Risk 2011", Lumension, 2011. [Online]. Available: http://www.lumension.com/Resources/Resource-Center/2010-State-of-the-Endpoint.aspx?rpLeadsourceID=2116. [Accessed Dec. 13, 2011].

[3] J. Pan, C.C. Fung, "Artificial Intelligence in Malware – Cop or Culprit?", The Ninth Postgraduate Electrical Engineering & Computing Symposium PEECS 2008, The University of Western Australia, Perth, Australia, 2008.

[4] W. Yan, Z. Zhang and N. Ansari, "Revealing Packed Malware", IEEE Security & Privacy, Issue5, Page 65 – 69, Sept. 2008.

[5] J.Rutkowska, "Subverting the Vista Kernel for Fun and Profit", Blackhat Briefings, 2006.

[6] L. Vaas, "Storm Worm Botnet Lobotomizing Anti-Virus Programs", eWeek.com, Oct. 24, 2007. [Online]. Available: http://www.eweek.com/c/a/Security/Storm-Worm-Botnet-Lobotomizing-AntiVirus-Programs/. [Accessed Dec. 13, 2011].

[7] D. Piscitello, “Conficker Summary and Review”, ICANN, May 7, 2010. [Online]. Available: https://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf. [Accessed Dec. 13, 2011].
[8] M. Brand, C. Valli and A. Woodward, “Malware Forensics: Discovery of the Intent of Deception”, Australian Digital Forensics Conference, 2010.
[9] J. Pan and C. C. Fung, “Boutique Malware – Custom made for e-business’, INCEB 2010, Thailand, Nov. 18, 2010.
[10] C. Valli and M. Brand, “The Malware Analysis Body of Knowledge (MABOK)”, Proceedings of the 6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2008.
[11] McAfee Labs, “McAfee Threats Report: First Quarter 2011”, McAfee, 2011.
[12] P. Mell, K. Kent and J. Nusbaum, “Guide to Malware Incident Prevention and Handling : Recommendations of the National Institute of Standards and Technology”, NIST Special Publication 800-83, National Institute of Standards and Technology, Nov. 2005.
[13] D. Goodin, “DDoS malware comes with self-destruct payload”, The Register, Mar. 9, 2011. [Online]. Available: http://www.theregister.co.uk/2011/03/09/ddos_bots_self_destruct/. [Accessed Dec. 13, 2011].
[14] Verizon, “2010 Data Breach Investigations Report”, Verizon Business, Jul. 28, 2010. [Online]. Available: http://www.verizonbusiness.com/go/2010databreachreport/. [Accessed Dec. 13, 2011].
[15] P. Y. Logan and S. W. Logan, “Bitten by a Bug: A Case Study in Malware Infection”, Journal of Information Systems Education, Vol. 14(4), 2003.
[16] C. Alexander, “The Timeless way of Building”, Oxford University Press, 1979.
[17] M. Schumacher and R. Roedig, “Security Engineering with Patterns”, Proceedings of the 8th Conference on Pattern Languages for Programs (PLoP 2001), Illinois-USA, Sept. 2001.
[18] J. Eckstein, J. Bergin and H. Sharp, “Patterns for Active Learning”, Proceedings of PloP 2002, 2002.
[19] K. Scarfone, T. Grance and K. Masone, “Computer Security Incident Handling Guide : Recommendations of National Institute of Standards and Technology”, NIST Special Publication 800-61 Revision 1, National Institute of Standards and Technology, Mar. 2008.
[20] J. H. Saltzer and M. D. Schroeder, “The Protection of Information in Computer Systems”, Communications of the ACM 17, 7, Jul. 1974.
[21] D. M. Kienzle, M. C. Elder, D. S. Tyree and J. Edwards-Hewitt, “Security Patterns Template and Tutorial”, Feb. 2002. [Online]. Available: http://www.securitypatterns.com/documents.html. [Accessed Dec. 13, 2011].
[22] T. Heyman, K. Yskout, R. Scandariato and W. Joosen, “An Analysis of the Security Patterns Landscape”, SESS ’07 Proceedings of the Third International Workshop on Software Engineering for Secure Systems, IEEE Computer Society, Washington DC, USA, 2007.
[23] N. Yoshiko, H. Washizaki and K. Maruyama, “A survey on security patterns”, Progress in Information, Special issue: The future of software engineering for security and privacy, No. 5, pp.35–47, 2008.
[24] Mitre, www.mitre.org.
[25] R. Naraine, “Microsoft Says Recovery from Malware Becoming Impossible”, eWeek, Apr. 4, 2006.
[26] R. Lemos, ‘Malware variants may have hit half-million mark’, Security Focus, Jan. 3, 2008. [Online]. Available: http://www.securityfocus.com/brief/655. [Accessed Dec. 23, 2011].
[27] D. May and P. Taylor, “Knowledge management with patterns”, Communications of the ACM, Vol. 46, No. 7, Jul. 2003.
[28] S. Kesh and P. Ratnasingam, “A Knowledge Architecture for IT Security”, Communications of the ACM, Vol. 50, No. 7, Jul. 2007.

[29] S. Fenz and A. Ekelhart, “Formalizing Information Security Knowledge”, ASIACCS ’09, Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, 2009.
[30] S. Barnum and G. McGraw, “Knowledge for Software Security”, IEEE Security & Privacy, Mar / Apr. 2005.