Fighting Fire with Fire – a Pre-emptive approach to Restore Control over IT Assets from Malware Infection

BY

Juin Yang Jonathan PAN

This thesis is presented for the degree of

Doctor of Information Technology of

Murdoch University

November 2012

DECLARATION

I declare that this thesis is my own account of my research and contains as its main content work that has not previously been submitted for a degree at any tertiary education institution.

Juin Yang, Jonathan PAN

ABSTRACT

Malware is a major threat as they induce multiple risks to infected organizations. Current Anti-Malware solutions meant to keep Malware away are challenged on how to keep the risks at bay effectively. When a Malware manages to penetrate an organization's defences, there is a need to effectively contain the Malware and retain control over the organization's IT assets before the risk escalates. In response, Malware Remediation is supposed to contain the effects of the Malware infiltration or outbreak. However Incident Responders face many challenges to contain the malice. One challenge is the logistics of how to coordinate a distributed and timely containment. Another is the need of an effective technique to defunct the Malware as they are able to overcome conventional countermeasures. The final challenge is how to maintain the level of effectiveness of the containment tools in the face of self-preservation attacks by the Malware. This research study evaluates the use of Malware techniques to address the three challenges as a part of Malware Remediation in order to restore control over the IT assets back to the organization.

In this thesis, the first proposition to the challenge of coordinating a distributed incident response plan is to use the distributed and coordinated characteristics of a command and control botnet. In order to validate this proposition, an agent based simulation model was developed to show that a good (non-malicious) botnet with its distributed and coordinated containment approach will result in faster Malware containment and reduce the effects of a Malware outbreak compared to conventional

manual containment techniques. The proposed solution to the second challenge is to use the offensive techniques used by Malware to defunct the targeted Malware. The evaluation is done through three experiments using three different offensive techniques against live Malware. One of the three experiments involved a smartphone Malware as this form of Malware is becoming increasingly prevalent in recent times. All three experiments showed that offensive techniques could effectively defunct the targeted Malware in the infected devices. The proposition to the final challenge is to adopt Malware resilient designs. The latter is used by Malware to protect themselves against Anti-Malware solutions and attempts to defunct them. The proposal is evaluated by conducting three experiments where a custom developed application that incorporated Malware resilience designs was attacked using Malware offensive techniques. All three experiments demonstrated that Malware resilient designs could aid Malware Remediation tool developers or Anti-Malware solution developers to protect their products against self-preservation attacks of Malware.

In order to facilitate the adoption of the three research proposals by Incident Responders, the last proposition in this thesis is to package the knowledge of using Malware techniques for Malware Remediation into Malware Remediation patterns. The latter uses a pattern template derived from common security pedagogical patterns. Samples of the Malware like Malware Remediation patterns are included in the thesis. The thesis concludes with a consideration into future research directions with respect to all the research proposals mentioned in the study.

SUMMARY OF CONTRIBUTION AND LIST OF PUBLICATIONS RELATED TO THIS THESIS

JOURNAL

1. ***From Chapter 3*** – J. Pan and C. C. Fung, "Agent Based Model to Simulate Coordinated Response to Malware Outbreak Within An Organization", International Journal of Information and Computer Security, 2012. (Accepted on September 2012 for Publication)

   Contribution to thesis – The paper details an Agent Based Model to simulate Malware Remediation efforts. This model is used to support the research proposition that Malware's distributed and coordinated characteristics (specifically that of the botnet) is an effective approach to remediate a Malware outbreak.

CONFERENCE PROCEEDINGS

1. ***From Chapter 6*** – J. Pan and C. C. Fung, "Pattern For Malware Remediation – A Last Line of Defence Tool against Malware in the Global Communication Platform", Accepted to be published in the Conference Proceedings of the International Telecommunications Society (ITS) 2012 Bangkok, November 2012.

   Contribution to thesis – The paper proposes the establishment of a Pattern template for Malware Remediation in order to address the adoption challenges

faced by Malware Incident Responders. This proposition is used in this thesis to translate Malware like remediation techniques into a pedagogically friendly format that will facilitate adoption by Malware Incident Responders.

2. ***From Chapter 2*** – J. Pan and C. C. Fung, "Boutique Malware – Custom made attacks on e-business", in Proceedings of the International Conference on E-Business (INCEB2010), Bangkok, Thailand, pp. 108 – 112, November, 2010.

   Contribution to thesis **–** The paper highlights a new form of Malware lurking that are customed built against targeted individuals or organizations. Such Malware are designed to circumvent deployed security defences. This study highlights the challenges faced by Malware Incident Responders in detecting and containing these Malware.

3. ***From Chapter 2*** – J. Pan and C. C. Fung and W. W. Koh, "Devious Chatbots – Interactive Malware with a Plot", in Progress in Robotics: FIRA RoboWorld Congress, Incheon, Korea, CCIS 44, pp. 110 – 118, August 2009.

   Contribution to thesis **–** The paper highlights a form of Malware lurking in the Internet with intelligent interactive capabilities to conduct social engineering attacks against its targets. This study highlights the heighten risk possibility that people will face prey to the attacks of Malware and in turn have their computers infected.

4. ***From Chapter 2*** – J. Pan and C. C. Fung, “Malware’s Impact on e-Business : they mean business !”, in the Proceedings of The Eighth Wuhan International Conference on E-Business, Wuhan, China, pp. 205 – 210, May 2009.

   Contribution to thesis **–** The paper highlights the disasterous impact of Malware to various stakeholders of e-Business or online industry. This study highlights the threat of Malware to organizations hence supporting the need for organizations to have preventive and remediative measures in place to mitigate against such risks.

5. ***From Chapter 2*** – J. Pan and C.C. Fung, “Artificial Intelligence in Malware – Cop or Culprit?” Proceedings of the Ninth Postgraduate Electrical Engineering & Computing Symposium (PEECS 2008), The University of Western Australia, Perth, Australia, pp. 181 – 184, November 2008.

   Contribution to thesis **–** The paper highlights the existence of Malware equipped with artificial intelligence capabilities to enhance its effectiveness to attack its targets and evade detection. This paper discusses the advancement of Malware technologies and challenges faced by Anti-Malware solution developers and Incident Responders to detect and contain Malware attacks.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

First and foremost, I would like to acknowledge my principal supervisor, Associate Professor Lance Chun Che Fung who has provided invaluable and wise guidance in the development of my research work, and more importantly, principles of good living. I would like to acknowledge my co-supervisor, Associate Professor Kevin Kok Wai Wong, who also gave me valuable advice in my doctoral study endeavour.

I would especially like to acknowledge my lovely wife, May, whose support and unconditional love gave me the drive to pursue this near impossible and long enduring dream.

Finally I would like to thank my organization and its management for their sponsorship and granted me the opportunity to pursue my doctoral study.

LIST OF FIGURES

LIST OF TABLES

LIST OF EQUATIONS

LIST OF DEFINITIONS

Agent Based Modelling or Agent Based Model	:	This is a simulation and modelling approach that provides the means to analyse a system's behaviour using "what-if" analysis under different conditions.
Anti-Malware	:	This refers to any product specifically designed to prevent Malware intrusion or to eradicate any instance of Malware detected. This term includes Anti-Virus products.
Defences or Security Defences	:	This refers to the Anti-Malware security solutions typically used by organizations. This entails Firewalls, Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Anti-Virus and associated solutions. This covers both enterprise deployment and endpoint security.
Good Botnet	:	Software based Incident Responders whose characteristics are similar to the Malware Botnet.
Incident Responders	:	This refers to the team, which is created when required or formally established, tasked to deal with the Malware incident within an organization. Other names for such a team is Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT). In this thesis, all such teams are referred to as Incident Responders.

Malware	:	A form of software that contains malicious code. The term Malware encompasses all forms of malicious software that includes but not limited to the Computer Viruses, Trojans and Botnets. It is a singular noun.
Malware Remediation	:	This is a security incident response activity that occurs after a successful Malware infiltration and existing security measures have limited abilities to contain or eradicate the intruder(s). This is also known as Malware containment. In this thesis, Malware Remediation is used instead of Malware containment.
Sink-holing	:	Redirecting all related or selected network traffic into a defined location as part of Malware Remediation. It is used to facilitate and aid investigation and containment of Malware's network traffic.

LIST OF ABBREVIATIONS

ADB	:	Android Debug Bridge is a versatile command line tool that provides the means to communicate with an Android emulator or connected Android-powered device
ABM	:	Agent Based Model
AMCM	:	Agent based Malware Containment Model
CAPEC	:	A publicly available and community developed list of cyber common attack patterns with schema and classification taxonomy by MITRE
CAPTCHA	:	Completely Automated Public Turing test to tell Computers and Humans Apart
C&C	:	Command and Control
CSIRT	:	Computer Security Incident Response Team
DDoS	:	Distributed Denial of Service
DIT	:	Doctor of Information Technology programme offered by Murdoch University, Australia
MAEC	:	A standardization language proposed by MITRE for encoding and communication details about Malware based on behaviours, artefacts and attack patterns
MITRE	:	MITRE Corporation is a non-for-profit organization tasked to work on technology development in the areas of public interest

OECD	:	Organization for Economic Co-operation and Development
P2P	:	Peer to peer
SIR	:	Susceptible-Infected-Recovered epidemiological model
USA	:	United States of America