

**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 customized 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 heightened 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

Declaration	ii
Abstract	iii
Summary of Contribution and List of Publications Related to This Thesis	v
Acknowledgements	xiii
List of Figures	xiv
List of Tables	xviii
List of Equations	xx
List of Definitions	xxi
List of Abbreviations	xxiii
1 INTRODUCTION	1
1.1 Summary Background	1
1.2 Problem Statement	3
1.3 Purpose of Study	5
1.4 Research Objectives	6
1.5 Research Approach	7
1.6 Significance of Research	8
1.7 Thesis Outline	9
2 BACKGROUND AND RELATED WORK	14
2.1 Problem – Malware Epidemic	14
2.1.1 Malware Risk to Organizations – Loss of Control	14
2.1.2 Malware’s Impact to Digital Economy	16
2.1.2.1 Direct Impact by Malware	17

2.1.2.2	Indirect Impact by Malware.....	18
2.2	Problem – Sophistication of Malware	19
2.2.1	Advanced Technologies in Malware Designs.....	19
2.2.1.1	Evasive Malware.....	19
2.2.1.2	Anti-forensic Malware	22
2.2.2	Targeted Malware Against Organizations	23
2.3	Problem – Faced by Existing Anti-Malware Solution.....	28
2.3.1	Defective Anti-Malware Defences	29
2.3.2	Anti-Malware Defences becoming Victims.....	30
2.4	Problem – Faced by the New Line of Defence	31
2.4.1	Coordination Challenge	31
2.4.2	Conventional Techniques Need Update.....	34
2.4.3	Remediation Tools: Another victim of Malware	35
2.5	The Research Needs.....	36
2.6	Related Work	39
2.6.1	Related Work on Coordinated Containment.....	39
2.6.2	Related Work on Offensive Containment.....	41
2.6.3	Related Work on Resilient Containment	42
3	DISTRIBUTED AND COORDINATED CONTAINMENT	44
3.1	Research Proposition	44
3.2	Related Biological Disease Research.....	44
3.3	Method of Evaluation	46
3.3.1	Modelling Containment	50
3.3.1.1	Agent based Modelling	51
3.3.1.2	Related Work on Agent based Containment Model	53
3.3.1.3	Agent based Malware Containment Modelling	56
3.3.1.4	Model Alignment to Existing Models.....	60

3.3.2 Quantitative Evaluation	65
3.3.2.1 Time Measurement	66
3.3.2.2 Data Loss Measurement.....	66
3.3.3 Experimentation.....	69
3.4 Analysis of Experiments	71
3.4.1 Analysis of Experiments Of Conventional Containment.....	71
3.4.1.1 Uncoordinated Containment	71
3.4.1.2 FIFO Containment	74
3.4.1.3 Prioritized Containment	76
3.4.2 Analysis of Malware Like Containment Experiments.....	78
3.4.2.1 Near Zero Latency Containment.....	79
3.4.2.2 Infectious Spread of Incident Responders	84
3.4.2.3 Botnet of Incident Responders.....	88
3.5 Discussion	93
3.6 Conclusion	95
4 OFFENSIVE CONTAINMENT	97
4.1 Research Proposition	97
4.2 Related Biological Disease Research Work	98
4.3 Analysis of Attack Patterns.....	101
4.4 Method of Evaluation	103
4.5 Analysis of Experiments	105
4.5.1 Analysis of Experiment 1.....	106
4.5.2 Analysis of Experiment 2.....	111
4.5.3 Analysis of Experiment 3.....	122

4.6	Discussion	130
4.7	Conclusion	132
5	RESILIENT CONTAINMENT	134
5.1	Research Proposition	134
5.2	Related Research Work on Biological Diseases	136
5.3	Method of Evaluation	138
5.4	Analysis of Experiments	140
	5.4.1 Analysis of Experiment 1.....	140
	5.4.2 Analysis of Experiment 2.....	145
	5.4.3 Analysis of Experiment 3.....	149
5.5	Discussion	154
5.6	Conclusion	155
6	PATTERN BASED MALWARE LIKE REMEDIATION	157
6.1	Problem	157
6.2	Research Proposition	160
	6.2.1 Patterns Introduction.....	160
6.3	Related Work	161
	6.3.1 Remediation Guide	162
	6.3.2 Knowledge Management in IT Security	162
	6.3.3 Security Patterns	163
6.4	Malware Remediation Pattern.....	165
	6.4.1 Pattern Set 1 – Non Malware Like Containment	167
	6.4.2 Pattern Set 2 – Malware Like Containment.....	169

6.5 Discussion	173
6.6 Conclusion	173
7 CONCLUSION	175
7.1 Malware Like Remediation.....	175
7.2 Considerations on The Propositions	176
7.3 Future Research Directions.....	177
7.3.1 Future – Agent based Malware Containment Model.....	177
7.3.2 Future – Distributed and Coordinated Containment.....	178
7.3.3 Future – Offensive Containment.....	179
7.3.4 Future – Resilient Containment	180
7.3.5 Future – Pattern Based Containment	180
7.4 Concluding Remark	181
Appendix A – Analysis of CAPEC Release 1.6	182
References.....	217

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

Figure 1.1: Thesis Structure Overview	9
Figure 2.1: Research Solution Illustration	38
Figure 3.1: Gene Therapy from U.S. National Library of Medicine	46
Figure 3.2: Agent Based Malware Containment Model Developed in Netlogo.....	48
Figure 3.3: Sample Netlogo Code of AMCM.....	49
Figure 3.6: AMCM's Inputs and Outputs.....	67
Figure 3.7: Epidemiological Chart for Uncoordinated Containment.....	73
Figure 3.8: Epidemiological Chart for FIFO Containment.....	75
Figure 3.9: Epidemiological Chart for Prioritized Containment	77
Figure 3.10: Epidemiological Chart for Near-Zero Latency (FIFO)	82
Figure 3.11: Epidemiological Chart for Near-Zero Latency (Prioritized).....	82
Figure 3.12: Epidemiological Chart for Infectious Containment (FIFO).....	86
Figure 3.13: Epidemiological Chart for Infectious Containment (Prioritized).....	86
Figure 3.14: Snapshot of AMCM - Good Botnet	90
Figure 3.15: Epidemiological Chart for Good Botnet (FIFO)	91
Figure 3.16: Epidemiological Chart for Good Botnet (Prioritized).....	92
Figure 4.1: Phage Therapy Illustration	100
Figure 4.2: Analysis of CAPEC (Release 1.6).....	102
Figure 4.3: AV Detects Malware	107
Figure 4.4: Malware Manually Terminated	108

Figure 4.5: Registry Manipulation.....	109
Figure 4.6: Malware Image Removal	109
Figure 4.7: Malware Removal Confirmed by AV	110
Figure 4.8: Malware's Listening Ports	113
Figure 4.9: One of the Registry Entries Changed By Malware	114
Figure 4.10: Internet Explorer's Configuration Alteration.....	114
Figure 4.11: Malware Executable Image	115
Figure 4.12: Metasploit Remote Access Payload Construction.....	116
Figure 4.13: Meterpreter Having Remote Access To Targeted.....	117
Figure 4.14: Remote Termination of Malware	118
Figure 4.15: Remote Removal Of Malware Image.....	119
Figure 4.16: Remote Registry Manipulation	119
Figure 4.17: No Malicious Listening Port	120
Figure 4.18: Malware's Registry Settings No Longer Exist	121
Figure 4.19: No Malware Residual Image.....	121
Figure 4.20: Trojan App for Android	124
Figure 4.21: Malware Detected by AV.....	125
Figure 4.22: Malware Resident In Android	125
Figure 4.23: Manual Termination of Malware's Background Service.....	126
Figure 4.24: Manual Termination Of Malware's Activity.....	127
Figure 4.25: Manual Removal Of the Trojan App.....	128
Figure 4.26: AV Scan To Confirm Removal Of Malware.....	129

Figure 5.1: Types of Malware Self Preservation Techniques.....	136
Figure 5.2: Pseudo Code To Protect Firewall.....	140
Figure 5.3: Custom Application For Malware Like Resilient Design.....	141
Figure 5.4: Metasploit Remote Access To Targeted Host.....	142
Figure 5.5: Warning Message About AV But Not Of Firewall.....	142
Figure 5.6: Disable Countermeasures Via Meterpreter	143
Figure 5.7: Warning Message About Firewall.....	143
Figure 5.8: Custom Application Reinstated Firewall	144
Figure 5.9: No Warning Message About Firewall.....	144
Figure 5.10: Pseudo Code To Protect Registry Settings.....	145
Figure 5.11: Registry Settings ('Flag') To Be Protected	146
Figure 5.12: Remote Manipulation Of Registry	147
Figure 5.13: Protective Restoration Of Manipulated Registry Setting	148
Figure 5.14: Registry Setting Value Preserved.....	148
Figure 5.15: Pseudo Code of Protection	149
Figure 5.16: Starting the ResilientTest.exe Application.....	150
Figure 5.17: Inclusion Of ResilientTest.exe into Meterpreter Script.....	151
Figure 5.18: Metasploit Found and Terminated Its Target.....	152
Figure 5.19: Application Restarted With a Random Process Name.....	153
Figure 5.20: Meterpreter Unable To Identify the Targeted Application	154
Figure 7.1: Botnet Characteristic Chart	178

LIST OF TABLES

Table 1.1: Research Need and Proposal	5
Table 1.2: Research Strategy	7
Table 2.1: Risk Analysis Of Control Over IT Assets	15
Table 2.2: Research Needs.....	37
Table 2.3: Research Needs And Proposal.....	37
Table 3.1: AMCM's Constants.....	56
Table 3.2: AMCM's Global Variables	57
Table 3.3: AMCM Parameters Used In Experiment Scenarios	58
Table 3.4: Parameters used in AMCM for Simulation of Data Loss Measurement	68
Table 3.5: Uncoordinated Containment Parameter Settings.....	72
Table 3.6: Uncoordinated Containment Test Results	73
Table 3.7: FIFO Containment Parameter Settings.....	74
Table 3.8: FIFO Containment Test Results	75
Table 3.9: Prioritized Containment Parameter Settings.....	76
Table 3.10: Prioritized Containment Test Results	77
Table 3.11: Near-Zero Latency Containment Parameter Settings	81
Table 3.12: Near-Zero Latency Containment Time Test Results	83
Table 3.13: Near-Zero Latency Containment Data Leakage Test Results	83
Table 3.14: Infectious Containment Parameter Settings.....	85
Table 3.15: Infectious Containment Time Test Results.....	87

Table 3.16: Infectious Containment Data Leakage Test Results	87
Table 3.17: Good Botnet Containment Parameter Settings	90
Table 3.18: Good Botnet Containment Time Test Results	92
Table 3.19: Good Botnet Containment Data Leakage Test Results	92
Table 5.1: Review Of Malware's Techniques	135
Table 6.1: Malware Remediation Pattern Sample 1	167
Table 6.2: Malware Remediation Pattern Sample 2	168
Table 6.3: Pattern of a Good Botnet	169
Table 6.4: Local Malware Image Removal Containment	171
Table 6.5: Resilient Guard Over Important Services	172

LIST OF EQUATIONS

Equation 3.1: SIR Epidemiological Equation.....	62
Equation 3.2: Data Leakage Equation	67

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