

VU Research Portal

Using Malware Analysis to Evaluate Botnet Resilience

Rossow, C.

2013

document version

Publisher's PDF, also known as Version of record

[Link to publication in VU Research Portal](#)

citation for published version (APA)

Rossow, C. (2013). *Using Malware Analysis to Evaluate Botnet Resilience*.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

E-mail address:

vuresearchportal.ub@vu.nl

Contents

Contents	I
Acknowledgements	III
Publications	V
1 Introduction	1
1.1 Problem Definition	1
1.2 Research Questions	2
1.3 Contributions	3
1.4 Thesis Outline	4
2 Background	5
2.1 The Malware Lifecycle	5
2.2 Botnet Architectures	6
2.3 Botnet Resilience	8
2.4 Malware Analysis	9
I Designing Sound Malware Experiments	11
3 Guidelines for Malware Experimentation	15
3.1 Introduction	15
3.2 Designing Prudent Experiments	17
3.3 Methodology for Assessing the Guidelines	21
3.4 Survey Observations	27
3.5 Experiments	34
3.6 Related Work	38
3.7 Conclusion and Discussion	39

4	Dynamic Malware Analysis with Sandnet	41
4.1	Introduction	41
4.2	System Overview	42
4.3	Dataset	44
4.4	Network Statistics Overview	44
4.5	DNS	47
4.6	HTTP	50
4.7	Related Work	60
4.8	Discussion	62
4.9	Conclusion	63
II	Botnet Resilience	65
5	Resilience Analysis of Malware Downloaders	69
5.1	Introduction	69
5.2	Malware Downloaders	70
5.3	Analysis of the Downloader Landscape	72
5.4	Downloader Resilience	78
5.5	Egg Acquisition and Analysis	84
5.6	Discussion	87
5.7	Conclusion	88
6	Resilience Analysis of Peer-to-Peer Botnets	89
6.1	Introduction	89
6.2	Preliminaries	90
6.3	Overview of P2P Botnets	92
6.4	P2P Botnet Populations	96
6.5	P2P Botnet Resilience	100
6.6	Discussion	106
6.7	Related Work	107
6.8	Conclusion	108
III	Epilog	109
7	Conclusions and Future Work	111
7.1	Conclusions	111
7.2	Future Work	112
	Bibliography	115
	Glossary	125
	Summary	127
	Samenvatting	129
	List of Figures	133
	List of Tables	135