

Peer-to-Peer bots Investigation using Distributed Honeypots

Karun Dambiec u4462988

Australian National University

COMP8760 Computer Science Project
Supervisor: Dr Warren (Huidong) Jin, NICTA



Bot

- A bot is an application or system that performs tasks when requested. For the purpose of this project, we only consider malicious bots.



Botnet

- A botnet is a group of bots which run on different systems and work together to achieve a malicious purpose for a botmaster.



IRC Botnet

- A botnet that uses a centralised form of control in this case an IRC server. It connects to the server and performs actions automatically as requested by the botmaster who sends messages to the IRC channel the bots are a member of.



Peer-to-Peer Botnet

- A peer-to-peer Botnet is a collection of bots which unlike a botnet do not have a centralised point of control, and act both as a client and server in a similar method to that of peer-to-peer filesharing applications[1].



LeurreCom.Org HoneyPot Project

- Consists of over 25 honeypots that are distributed.
- In operation and collecting data since 2003.
- Non-Disclosure Agreement
- <http://www.leurrecom.org>



Goals

- To investigate new trends in the behaviour of peer-to-peer botnets using the data from the honeypot project.
- To analyse peer-to-peer bots.
- The project will be a hybrid research/implementation project.



Timetable

Week	Dates	Activities
1	21/7-27/7	Initial Meeting Define Research to be undertake Begin Review of Background Literature Begin Initial Presentation
2-3	28/7-3/8	Literature Review Data Exploration Finalisation of Study Contracts
4	11/8-17/8	Initial Project Presentation Continued Data Exploration Continuation of Literature Review
5-7	18/8-7/9	Research
8-10	8/9-28/9	Research
Mid Semester Break	29/9-12/10	Research Implementation
11	13/10-19/10	Evaluation of Results
12-13	20/10-2/11	Final Report Writeup Final Presentation Submission of Final Report



References



Julian B. Grizzard, Vikram Sharma, Chris Nunnery, Brent ByungHoon Kang, and David Dagon.
Peer-to-peer botnets: overview and case study.
In HotBots'07: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, pages 1–1, Berkeley, CA, USA, 2007. USENIX Association.



Acknowledgements

- NICTA for allowing me to visit from July 2008 November 2008.
- SGNNet Honeypot Project Participants



Questions/Comments?

