



The Australian National University
Faculty of Engineering and Information Technology
Department of Computer Science

Peer-to-Peer Bots investigation based on Distributed Honeypots

Karun Dambiec
Supervisor: Dr Warren (Huidong) Jin, NICTA

This is the project plan for the COMP8760 Computer
Science Project (Semester 2, 2008)

August 2008

Background

Peer-to-peer botnets are becoming an increasing threat to the security of computer networks and systems. Because of the number of bots involved in recent botnets, and as a result the amount of bandwidth that could be potentially utilised, a distributed attack on an organisations computer network could severely affect an organisations ability to function and impact it financially.

We introduce the concepts of a bot, botnet, IRC botnet, peer-to-peer botnet and honeypots. We provide a brief background of the honeypot project from which the data will be sourced.

Bot

A bot is an application or system that performs tasks when requested. For this project we only consider bots that are malicious.

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 and 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 an IRC botnet do not have a centralised point of control, and act aboth as a client and server in a similiar manner to that of peer-to-peer filesharing applications[Grizzard et al. 2007].

Honeypot

A honeypot is a system which collects any data that has been sent to it over a network, and it allows us to record information about any unauthorised traffic or attempts to attack a network[Mokube and Adams 2007]. We can then analyse the data from the honeypot at a later date to determine trends in the behaviour of peer-to-peer botnets, and to find methods of detecting attempted intrusions in order to prevent them.

SGNet Honeypot project

SGNet is a worldwide honeypot project, consisting of a distributed network of 25 honeypots with multiple participants. It uses ScriptGen technology to allow a high level of interaction with its attackers, so it can collect more detailed information than the LeurreCom honeypot project[Leita and Dacier 2008].

Problem Description

We have access to the proprietary SGNet honeypot database. This project is a hybrid research/implementation project.

Initially we will focus on understanding the SGNet database, and what information we can get from it. Next we will select a appropriate data mining tool depending on our understanding of the data and the timeline.

We will then investigate new trends in the behaviour of peer-to-peer botnets using data from the SGNet honeypot project. We will analyse the peer-to-peer botnet data from the honeypot project. We will then evaluate our results, and use the data to verify any new behaviour of peer-to-peer botnets if we discover some new behaviour in the dataset.

The approach we take to this project will change depending on what we discover about the data.

Deliverables

We will deliver the following items by the dates specified in the proposed timetable:

1. Initial Presentation
2. Project Plan
3. Final Presentation
4. Final Report

Proposed Timetable

We propose the following timetable for this project:

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

We will initially define the research that will be undertaken, review background literature, perform exploration of the data provided by the SGNet Honeypot project, research and select the data mining tool to be used, analyse the data for trends in peer-to-peer botnets, evaluate our results and then finalise our report and presentastion.

References

- GRIZZARD, J. B., SHARMA, V., NUNNERY, C., KANG, B. B., AND DAGON, D. 2007. 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* (Berkeley, CA, USA, 2007), pp. 1–1. USENIX Association. (p.1)
- LEITA, C. AND DACIER, M. 2008. Sgnet: A worldwide deployable framework to support the analysis of malware threat models. *edcc-7 0*, 99–109. (p.2)
- MOKUBE, I. AND ADAMS, M. 2007. Honeypots: concepts, approaches, and challenges. In *ACM-SE 45: Proceedings of the 45th annual southeast regional conference* (New York, NY, USA, 2007), pp. 321–326. ACM. (p.1)