Master’s Thesis:

Analysis of Internet Relay Chat Usage
by DDoS Zombies
for Stéphane Racine <sracine@ee.ethz.ch>

1 Introduction

DDoS in general

Distributed Denial of Service (DDoS) attacks are a threat to Internet services ever since the widely published attacks on ebay.com and amazon.com in 2000. ETH itself was the target of such an attack six months before these commercial sites where hit. ETH suffered repeated complete loss of Internet connectivity ranging from minutes to hours in duration. Massively distributed DDoS attacks have the potential to cause major disruption of Internet functionality up to severely decreasing backbone availability.

Internet Relay Chat and DDoS

It is well known that Internet Relay Chat (IRC) is used not only by humans for chatting but can also serve as a means to send commands to malicious programs (the “bots”) running on compromised hosts (the “zombies”). A person (the “master”) can log into a specific IRC channel, which hundreds or even thousands of bots are listening to, and issue a command such as e.g. `attack <IP address>` that is received and executed by the bots. In this way, the IRC service can be abused to coordinate and launch DDoS attacks.

The DDoSVax Project

In the joint ETH/SWITCH research project “DDoSVax”\(^1\) abstract Internet traffic data (Cisco Netflow) is collected at all border gateway routers operated by SWITCH. This data contains information about which Internet hosts were connected to which others and how much data was

\(^1\)See http://www.tik.ee.ethz.ch/~ddosvax/
exchanged over which protocols.

For this thesis the DDoSVax research team has established a contact to an administrator of a frequently used IRC system that is temporarily located in the SWITCH network.

2 The Task

The task of the student is split in four major subtasks: IRC analysis, IRC-based DDoS attacks, Netflow-based IRC abuse detection, and DDoS attack countermeasures.

IRC analysis

The IRC service and protocol must be thoroughly understood and analysed. We recommend to read the IRC protocol specification RFC, to investigate various IRC clients\(^2\), to connect to various IRC servers and to listen as well as to participate in many IRC channel discussions.

A rough estimation on the IRC user community size and a classification should be made to judge the importance of this service.

IRC-based DDoS attacks

Related work about IRC abuse for DDoS attacks will be considered and a survey written.

By analyzing the logs and parameters of a specific IRC system, channels that are abused by bots will have to be identified and their behaviour will be observed and various methods for detection of such channels will be proposed.

Netflow-based IRC abuse detection

The IRC traffic between IRC clients outside the SWITCH network and the IRC server within the SWITCH network, which is investigated in this thesis, crosses one of SWITCH’s various border gateway routers. As the DDoSVax project collects Netflow traffic data at those border gateway routers, such IRC traffic data is available for analysis.

Before any analysis can be done, the student must understand the structure and limitations of Netflow data as well as the data capturing process used in the DDoSVax project. Already existing tools for data analysis should be considered.

With the results of the previous steps, various algorithms to extract and analyse IRC traffic data and especially such data that belongs to possibly abused IRC channels will have to be developed and thoroughly tested for effectiveness. The result will be one or more implemented and tested “IRC attack detection signature” that can detect IRC-based DDoS attack (preparation) traffic in Netflow traffic data.

\(^2\)mIRC is a very commonly used IRC client
IRC-based DDoS attack countermeasures

Assuming that we can detect suspicious IRC traffic in near-realtime, countermeasures that could be applied to routers and/or IRC systems will be proposed (on a rather conceptual basis) and their effectiveness evaluated.

3 Deliverables

The following results are expected:

1. IRC survey A short survey that explains current IRC services (importance, user group, specialities, use and abuse).
2. IRC-based DDoS attack survey A short but precise survey that summarizes IRC-based DDoS attacks already known in the literature.
3. IRC Attack Detection Signatures Description, implementation, and validation of various algorithms that detect IRC-based DDoS attack (preparation) traffic in Netflow traffic data.
4. Countermeasures Propositions of countermeasures to IRC-based DDoS attacks in a rather conceptual way. These descriptions will be part of the main documentation.
5. Master’s Thesis Documentation A concise description of the work conducted in this thesis (task, related work, environment, results and outlook). The two surveys as well as the descriptions of detection signatures and countermeasures are part of this main documentation.

Further optional components are:

- Graphical plots of aggregated statistics over time extracted from Netflow data
- Near-real-time implementation of attack signatures (instead of offline analysis) for our DDoSVax UDP framework
- Generalizations (not IRC-specific) of the detection algorithms and countermeasures proposed

Documentation and Presentation

A documentation that states the steps conducted, lessons learnt, major results and an outlook on future work and unsolved problems has to be written. The code should be documented well enough such that it can be extended by another developer within reasonable time. At the end of the thesis, a presentation will have to be given at TIK that states the core tasks and results of this Master’s thesis. If important new research results are found, a paper might be written as an extract of the thesis and submitted to a computer network and security conference.
Dates

This Master's thesis starts on Oct. 27th, 2003 and is finished by April 26th, 2004. It lasts 26 weeks in total.

Supervisors

Thomas Dübendorfer, duebendorfer@tik.ee.ethz.ch, +41 1 632 71 96, ETZ G64.1
Arno Wagner, wagner@tik.ee.ethz.ch, +41 1 632 70 04, ETZ G64.1