OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

MASTERTHESIS

Valentin Brandl

Organized Crawling of P2P Botnets

October 14, 2021

Faculty:	Informatik und Mathematik
Study Programme:	Master Informatik
Supervisor:	Prof. Dr. Christoph Skornia

Foo Bar baz lel

Contents

1 Introduction

A botnet describes a network of connected computers with some way to control the infected systems. In classic botnets, there are one or more central coordinating hosts called command and control servers (C2 servers). These C2 servers could use anything from internet relay chat (IRC) over hypertext transfer protocol (HTTP) to Twitter to communicate with the infected systems. The infected systems can be abused for a number of things, *e.g.* distributed denial of service (DDoS) attacks, stealing data from victims, as proxies to hide the attackers identity, send spam emails ...

Analyzing and shutting down a centralized botnet is comparatively easily since every bot knows the IP address, domain name, Twitter handle, IRC channel ... the C2 servers are using. A targeted operation with help from TODO, hosting providers, domain registrars and platform providers could shut down or take over the operation by changing how requests are rooted or simply shutting down the controlling servers/accounts.

A number of botnet operations were shut down like this and as the defenders upped their game, so did attackers — the idea of peer-to-peer (P2P) botnets came up. The idea is to build a decentralized network without single points of failure where the C2 servers are. In a P2P botnet, each node in the network knows a number of it's neighbours and connects to those, each of these neighbours has a list of neighbours on his own, and so on.

List of Figures

Acronyms

C2 server command and control server

DDoS distributed denial of service

HTTP hypertext transfer protocol

IRC internet relay chat

P2P peer-to-peer

Erklärung

1. Mir ist bekannt, dass dieses Exemplar der Masterthesis als Prüfungsleistung in das Eigentum der Ostbayerischen Technischen Hochschule Regensburg übergeht.
2. Ich erkläre hiermit, dass ich diese Masterthesis selbstständig verfasst, noch nicht anderweitig für Prüfungszwecke vorgelegt, keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie wörtliche und sinngemäße Zitate als solche gekennzeichnet habe.

Ort, Datum und Unterschrift

Presented by:	Valentin Brandl
Student ID:	3220018
Study Programme:	Master Informatik
Supervisor:	Prof. Dr. Christoph Skornia