Edinburgh Napier University

Botnet Detection and Mitigation in ISP Environments

Author:
Tobias Kickinger

Supervisor:
Bruce Ramsay

*Submitted in partial fulfilment of
the requirements of Edinburgh Napier University
for the Degree of
Master of Science in Advanced Security and Digital Forensics*

School of Computing

August 2015

Authorship Declaration

I, Tobias Kickinger, confirm that this dissertation and the work presented in it are my own achievement.

Where I have consulted the published work of others this is always clearly attributed;

Where I have quoted from the work of others the source is always given. With the exception of such quotations this dissertation is entirely my own work;

I have acknowledged all main sources of help;

If my research follows on from previous work or is part of a larger collaborative research project I have made clear exactly what was done by others and what I have contributed myself;

I have read and understand the penalties associated with Academic Misconduct.

I also confirm that I have obtained **informed consent** from all people I have involved in the work in this dissertation following the School's ethical guidelines.

Signed: Tobias Kickinger

Date: 16th August 2015

Matriculation No: 40113605

Data Protection Declaration

Under the 1998 Data Protection Act, The University cannot disclose your grade to an unauthorised person. However, other students benefit from studying dissertations that have their grades attached.

Please sign your name below one of the options below to state your preference.

The University may make this dissertation, with indicative grade, available to others.

____

The University may make this dissertation available to others, but the grade may not be disclosed.

Tobias Kichninger

The University may not make this dissertation available to others.

____

Abstract

Botnets are a computer security threat that evolved over the last few years. Typically, botnets are used for sending large volumes of spam emails, performing coordinated network-based attacks, conducting identity theft or financial fraud. Internet service providers (ISPs) can play a major part in fighting botnets, as they are able to detect and monitor botnet communication in their networks. It is also in their self-interest to implement measures against botnets, as botnet threats lead to significant risks for business operations.

Because risks for ISPs have not been systematically analysed yet, this thesis aims at a methodological risk analysis of botnets to enable an ISP to decide on measures to minimise threats for its infrastructure. It answers the questions which threats an ISP faces from botnets and which specific requirements and restrictions for botnet detection and mitigation exist for an ISP environment.

After performing a literature review of relevant work, this thesis adopts the risk assessment approach of the ISO/IEC 27005:2011 standard and applies it to an ISP environment facing botnet threats. The process steps are applied to determine the specifics of botnets, to describe requirements and limiting factors of the ISP environment, and to identify and analyse the resulting risks. The subsequent qualitative evaluation of these risks regarding likelihood and business impact is discussed to show which risks are most threatening for ISPs.

The identified top-rated risks of this work are: potential impact on ISP service quality and performance, total loss of important services, getting blacklisted which impairs legitimate traffic, non-compliance of detection or mitigation measures, and insufficient performance or scalability of measures.

This work concludes with a discussion of the risk implications for ISPs and states possible counter-measures. The results clearly show strong incentives to act on these risks, however, still require a subsequent assessment of business value.

Contents

List of Figures

List of Tables

Acknowledgements

First of all, I would like to sincerely thank my supervisor, Bruce Ramsay, for his professional advice, academic support and his untiring patience throughout this thesis. In addition, my thanks go to Bill Buchanan for his constructive feedback and for being my second marker.

Particularly, I would also like to thank my superiors at my employer, *M-net Telekommunikations GmbH*, a German ISP. This study would not have been possible without their flexibility and concessions. Also, I am grateful to my colleagues for the professional discussions and the exchange of insights regarding ISP environments and botnets.

Finally, I want to express my deep gratitude to my wife who has constantly supported and, despite all the highs and lows, has unswervingly encouraged me in the last few years—*thank you.*

Chapter 1

Introduction

1.1 Context and Background

Botnets are a computer security threat that evolved over the last few years. A botnet consists of compromised computers running malicious software and, without the knowledge of their owners, are under the control of one rogue entity, the so-called botmaster. As a result, this remote attacker controls the resources of hundreds, sometimes even hundreds of thousands of computers, i.e. processing power, storage and network bandwidth, in order to perform illegal tasks. Typically, botnets are used for sending large volumes of spam emails, performing coordinated network-based volume attacks (distributed denial-of-service, DDoS), hosting pirated media and conducting identity theft or financial fraud.

Internet Service Providers[1] can play a major part in fighting botnets, as they are able to detect and monitor botnet communication in their network. Additionally, it can also be in the interest of an ISP to implement measures as self-protection, as botnet-initiated DDoS attacks can have a major performance impact on the network infrastructure. Furthermore, high volumes of spam could impair the reputation of the ISP, its customers and its IP address space, and especially the latter may obstruct legitimate email transfers.

[1] Usage in this thesis: *singular* ISP, *plural* ISPs

Van Eeten and Bauer (2008) performed a study regarding incentives to fight malware and conclude that, especially for ISPs, there are only very few incentives to act against malware, because, according to the authors, the main incentive for ISPs are costs. In a later study, Van Eeten et al. (2010) state that ISPs operate in a contradictory incentive structure between forces trying to mitigate malware while others try not to. To clarify the situation if there are really only few incentives for ISPs to fight botnets, this thesis gives this issue further attention in order to analyse if botnet-induced risks exist and if they represent additional incentives for ISPs or not.

1.2 Aims, Objectives and Research Questions

This thesis aims at a methodological risk analysis of botnets in order to enable an ISP to decide on measures to minimise threats for the ISP's infrastructure.

The main research questions to be answered are:

- Which threats does an ISP face that result both from botnets in general and from botnet-infected customer systems?
- What are the specific requirements and restrictions for botnet detection and mitigation within an ISP environment?

For this thesis, the following objectives were defined in order to support the aims:

1. Perform a literature review by investigating and reviewing relevant literature in the fields of botnets, ISP threats and risk assessment schemes.
2. Decide upon the risk assessment approach and consider the overall methodology that is going to be used.
3. Perform an extensive risk assessment of botnet threats on ISP environments by identifying and evaluating associated risks.

4. Discuss the results from the risk assessment, how these can be mitigated and which recommendations for ISPs result.
5. Evaluate the outcome of the thesis as well as the applied methods and techniques and appraise the contributed value of the results.

1.3 Contributions

In order to answer the aforementioned research questions, this thesis delivers a threat description of botnets and botnet-infected customer systems from an ISP perspective including a detailed risk analysis; a structured analysis of ISP-specific factors, requirements and restrictions for botnet detection and mitigation; and a critical evaluation of the results considering the specific environment and recommendations for further implementation.

1.4 Motivation for this Work

The author of this thesis works at a mid-sized ISP as security engineer and holds responsibility for the overall security of the customer-facing wide area network (WAN) and in this position, he is confronted with the effects of botnets on a daily basis. However, to decide upon an adequate strategy to cope with botnets in such an environment, a comprehensive view on the threats and risks is required in order to focus and prioritise activities—and apparently, such a comprehensive analysis for this specific scenario was not available so far. This understanding is also backed by Plohmann et al. (2011, p. 4), who demand “a view divided into stakeholder perspectives” instead of a generalised threat assessment of botnets.

Although extensive research has been performed (and still continues) by others in this field to analyse single botnets, to detect certain characteristics or to infiltrate and shutdown certain botnets, a fundamental analysis of the threats of botnets and the evolving risks for an ISP—including a structured identification of issues as well as the specific requirements and limiting factors of such an environment—is still missing which is why this work has been conducted.

1.5 Structure of this Work

This thesis is divided into six chapters which are structured as follows:

Chapter 1. *Introduction* This chapter describes the initial project idea, the aims and objectives as well as motivation for the thesis.

Chapter 2. *Literature Review* This chapter gives a comprehensive review of relevant academic literature in this field and presents different views on botnets, their history and threats to impart a well-founded background of the topic.

Chapter 3. *Methodology* This chapter defines the methodical approach of the risk assessment to achieve the goals of this work. The methodology is derived from the established international standard ISO/IEC 27005:2011 for information security risk management.

Chapter 4. *Analysis and Results* This chapter presents the results of the analysis, covering a description of the risk context of botnets in ISP environments, a structured analysis of threats and derived risks and an evaluation considering the specific factors of the object of study.

Chapter 5. *Discussion of Results* This chapter discusses the analysed risks by considering them both individually and in the wider context and states implications for ISPs. Additionally, the overall work is critically evaluated, including the applied methods and techniques.

Chapter 6. *Conclusions* This final chapter concludes the thesis by discussing the overall achievements and by stating possible future work.

Chapter 2

Literature Review

The modern society has become so much digitalised that online networks and computer technology have become part of daily life. Computers are currently being used in different fields including research, medicine, finance, business and education. Despite the countless benefits associated with the use of computer systems, use of computer systems is plagued with various security risks which are discussed by Akkaladevi and Katangur (2010). Computer systems and networks are always under constant risk of threats posed by botnets, worms and viruses.

As far as the author is aware, no other methodical risk assessments of the given scenario has been performed so far. Although substantial work regarding botnet threats from a business value perspective has been performed by West (2008), neither a comprehensive botnet risk analysis was performed on a technical view nor the ISP environment was considered. Additionally, Elliott (2010) discusses some botnet threats and performs a mapping of incident scenarios regarding botnets to derive certain risks, however, those results are on a very high abstraction layer and have only limited significance for this thesis.

At first, to approach the problem, a distinction between different malware categories is given.

2.1 Types of Malware

Over the last decades, malware was subject to continuous evolution and can be divided into groups by its functional principle. According to Aycock (2006, chap. 2), there is no universal or conclusive definition of the terms, however a generally accepted one which is discussed in the following sections. The different kinds of malware show different characteristics regarding its propagation approach and attack vector. Typically, all malware types share the common goal to either stay undetected or to make its removal as hard as possible.

Computer Virus

A computer virus (or simply *virus*) is a type of malware whose major property is self-replication into other executable files. In order to exist and similar to its pathogen equivalent, a virus requires a *host* in terms of an executable file as a basis to copy itself into other files. The propagation to other systems happens by exchange or transfer of infected files, e.g. via mobile storage media or via network shares.

Computer Worm

A computer worm shares some characteristics with a virus, e.g. its self-replicating nature. However, a worm propagates itself actively to other computers, typically over a network and without relying on a *host* (i.e. infected) file. Instead, worms exploit network-based vulnerabilities in order to infect other systems. As stated by Plohmann et al. (2011, sect. 1.1), a worm does not necessarily contain routines to harm the infected system. There exist some worms with the sole purpose to spread itself and, if applicable, some sort of payload or establish a communication channel to a central control entity.

Trojan Horse

Similar to its historic reference, a Trojan horse pretends to perform a legitimate, benign task while secretly it executes malicious code. Typically, a Trojan horse tries to exfiltrate data (see *Spyware* description) or make the system part of a botnet (see *Botnet* description) as part of its actual purpose (Aycock, 2006, sect. 2.1).

Spyware, Keylogger and Sniffer

The main objective of this kind of malware is to record sensitive information and to deliver it to the attacker (so called *data extraction*). This goal is achieved by functions to record key strokes (*key logging*) or to eavesdrop on network communication (*sniffing*). The gained data is then exfiltrated over the Internet via more or less covert channels. Often, such functionality is included in or combined with other types of malware. However, it can also occur independently (Aycock, 2006, sect. 2.1).

Rootkit

A rootkit applies several invasive mechanisms to avoid detection and removal of the malware by placing and hiding itself deeply within the operating system, boot sector or even BIOS or (U)EFI. To achieve this, it uses special privileges or functions to stay unrecognised. Due to the nature of these functions, the removal of rootkits is complicated (Plohmann et al., 2011, sect. 1.1).

Botnet

Bots, also called *zombies* or *drones*, provide the basis for botnets and represent malware-infected systems. A botnet malware implements the functionality of several other described malware types in order to compromise computer systems and to abuse their resources. This can include both propagation approaches of worms, the invasive mechanisms of rootkits and data extraction techniques of spyware. Afterwards, the bot connects to a controlling entity and awaits further instructions. The so arising cluster of similar bots of a specific malware is called *botnet* and can reach sizes of thousands or even millions of infected systems (Plohmann et al., 2011, sect. 1.1). Due to the possibility of a coordinated, focussed usage of the bots' resources (CPU, network bandwidth, etc.), various purposes for botnets arise.

2.2 History of Botnet Development

Dunham and Melnick (2008) define a bot as software with the capability to manipulate computers. Generally, bots tend to repeat their actions. These actions may be destructive or geared towards perpetrating other destructive actions. Livingood et al. (2012) define a malicious bot as "a program that is surreptitiously installed on a system in order to enable that system to automatically (or semi-automatically) perform a task or set of tasks" under the control of the botmaster, i.e. a remote administrator.

A botnet is a collection of bots that are typically under the same remote administrator and a common or shared goal. When a botnet penetrates a network, the remote administrator may be able to control the entire network. Most botnets use command and control servers (C&C): Internet-connected computers that allow hackers to send information from remote locations. Early bots employed IRC (Internet Relay Chat) to communicate, this made it easy to deactivate and terminate them once detected. With time, newer generations of bots have emerged. These newer bots utilise sophisticated command and control methods that make them more resistant to deactivation.

Botnets gained popularity in the late 1990s largely due to the popularity of "Pretty Park" and "Sub7". These malwares distributed the possibility of infecting a machine using a malware and using the malware to connect to others via a communication channel—IRC in the case of these two malwares (Goranin et al., 2012). The realisation that malwares could utilise interconnectivity of computers led to significant strides in the design and implementation of botnets. The first major global botnet threat utilised TCP in attacking computers and transmitting commands (Akkaladevi and Katangur, 2010). A good example of such botnets is "Agobot" which was highly efficient in terms of speed and reach. Agobot delivered payloads that led to the installation of backdoors that could be used to disarm anti-virus software (Dunham and Melnick, 2008).

By 2003, hackers were exploring new modes of attack geared towards avoiding detection. This led to the realisation of the vulnerabilities of IRC connections. A botnet using this type of connection could be eliminated by a simple blacklist, as observed by Bauer and Van Eeten (2009). This led to exploration into the use of peer-to-peer (P2P) systems. The "Waledac" botnet utilised zombie computes to link the different bots in the botnet (Al-Ahmad and Al-Ahmad, 2014). Modern botnets even use social media networks such as Twitter and Facebook to control the computers hosting the bots, a fact analysed by Goranin et al. (2012). Social media is currently one of the most attractive medium for botnet hackers due to its global reach.

Modern botnets can attack machines and affect traffic into and out of a target system. DDoS attacks are a modern reality made possible by the distributed nature of botnets. A spam botnet named "Rustock" has been developed that affected up to 41% of its target destination (Tiirmaa-Klaar, 2013). Some of the modern botnets have the ability to hide. For example, "Cutwail" botnet had backup connections which allowed individual bots to create new hostnames to be used by their control server daily (Dunham and Melnick, 2008). This design was first utilised by "Conficker" botnet in 2008. Unlike the Cutwail botnet, the Conficker botnet generated over fifty thousand names daily. This botnet affected more than six million computers. Cutwail and Conficker botnets have affected more computer systems than any other botnet over the last decade.

2.3 Botnet Features

The characteristics of botnets are typically used in their classification. Thus, it is possible to classify botnets based on their different features and characteristics.

Structure is one of the most discussed aspect of botnets. The structure of a botnet defines its connectivity patterns, specifically between individual bots and the control server. Botnets typically use C&C networks for communication. In one architecture, not all bots have to be connected to a C&C. The bot that is connected to the C&C can control other bots and affected machine through continued monitoring of instructions and operations (Akkaladevi and Katangur, 2010). This structure has the benefit of simplicity; however, it is vulnerable to single point of failure. The whole botnet may collapse when the C&C stops operations. This vulnerability is the motivation for P2P botnets.

Peer-to-Peer botnets use a decentralised structure, as discussed by Asghari (2010). As a result, the existence of the botnet does not depend on a C&C server or an individual bot. Under this structure, every bot keeps connections to other bots to facilitate continuous interchange of information and commands. This structure is associated with improved ease of information interchange and high efficiency in the execution of commands. Zeus, a major botnet that targets machines running on Windows operating systems is an example of a botnet that utilises this structure (Dunham and Melnick, 2008).

The methodologies used in exchanging information between bots over network protocols can also be used to classify botnets. IRC-oriented botnets use the IRC network protocol to communicate. This type of botnets is highly reliant on the Internet for the relay of information. In IRC-oriented botnets, every bot is commanded via an IRC channel whereas all commands typically come from the IRC server (Stinson and Mitchell, 2008). Other botnets tend to utilise independent domains. In general, TCP is widely employed for communication within botnets.

Another approach to characterise botnets is based on messaging services. This type of characterisation is based on the medium via which commands and information are received and exchanged. IM-oriented botnets receive their commands via instant messaging (IM) servers. Web-based botnets are another category that receive commands via the World Wide Web infrastructure. These types of botnets establish connections to web servers thereby allowing them to send and receive information (Akkaladevi and Katangur, 2010). Use of web servers makes the management of such botnets very easy for hackers. The next category of botnets send and receive information via social media networks, for instance Twitter. This botnet architecture requires the involvement of social media users. Social media users are sent fake links which when clicked allows the hackers to exploit the user's system (Goranin et al., 2012). Most of the bots in this category make use of application protocols. The architecture and the protocols utilised by these bots make it hard for users and ISPs to detect its existence. Botnets in this category include "Flashback" which was intended for Twitter users.

Size can and has been used widely in the categorisation of botnets. Size is defined as the number of participating bots in a botnet. Large botnets have multiple bots that aid in the spread of commands whereas small botnets have few bots (Goranin et al., 2012). The power of these botnets is typically affected by their sizes. Larger botnets often are able to attack large or multiple targets. In contrary, smaller botnets are typically only able to launch attacks on a smaller target or fewer systems because of their restricted power. Therefore, the size of a botnet influences its range of transmission and the number of computers it can affect.

The objectives and intentions in creating a botnet differs across different hackers. The diversity in the objectives makes it possible to classify botnets according to their intentions. Gassen et al. (2013) state that botnets which are used for sending spam are typically operated with the intention of gathering sensitive information from its target systems. The "Koobface" botnet which has affected nearly 3 million computers so far, is one example for such botnet type. Some hackers develop botnets whose sole purpose is to steal private information which hackers can then use for their financial benefits. Bots in such botnets are typically instructed to scan Internet platforms to identify financial details or other private information that can be used for financial gain (Antonakakis et al., 2012). “Zeus” is an example of such botnets and further discussed by Dunham and Melnick (2008).

Mobile botnets are a recent development. Developments in the mobile phone industry have allowed for the use of technologies that can be utilised for transmission of malicious applications across mobile networks. Mobile botnets typically transmit malicious applications or code across mobile phone users. In 2011, over 40 000 mobile phones shared communication via C&C servers (Akkaladevi and Katangur, 2010). In China, millions of mobile phones have been affected by botnets that utilise popular applications. The approach employed by mobile botnets to allow for the transmission of information and commands is the same as in computers. The lack of robust security mechanism for mobile phones and their increasing processing capabilities have made mobile botnets an area of interest for hackers.

2.4 Network Level Detection of Botnets

The growing complexity of botnets especially in structure makes it hard to block or blacklist their information pathways. This had led to suggestions that the primary network defence against bots should move from individual users to Internet service providers (Stalmans and Irwin, 2011). Various DNS traffic-monitoring approaches have been attempted in efforts aimed at detecting malicious activities (Van Eeten et al., 2010). The passive analysis of recursive DNS traces led to the detection of malicious fast-flux service networks, as described by Holz et al. (2008)—fast-flux service networks will be discussed again in the analysis part of this work. IP addresses associated with the affected domains changed rapidly and were from dissociated networks. These features can then be used in the creation of heuristic classification models that are then used in the detection of such botnets

(Holz et al., 2008). This approach revealed that fast-flux botnets can be detected accurately using the number of different autonomous system numbers associated with domains and the number of distinct A-records (Stalmans and Irwin, 2011). Moreover, botnet controllers do not easily hide this information.

The second approach that can be used by ISPs is targeting the end goals of the botnets. Botnets that generate email spam can be handled using ISP level traffic filtering. This type of botnet requires sending spam to different network users to achieve its end goals which is stealing information from the network users. Reducing or eliminating the volume of spam that reach the end users can therefore reduce the effectiveness of these botnets. In Australia, significant improvements have been made in reducing the effectiveness of botnets via ISP level filtering (Stalmans and Irwin, 2011). Machine learning techniques and even statistical techniques can be used in the prediction and classification of traffic.

Stalmans and Irwin (2011) proposed the use of a system that can examine DNS query responses from the perspective of the ISP's DNS servers. The proposed system would look for features that have been identified in previous studies such as the number of A-records and TTL. This information would then be used in the classification of domains as either malicious or non-malicious. A user that queries a domain that has been classified as malicious would then receive a modified response such as "domain not found". This approach would prevent bots from contacting their C&C servers while allowing users to access legitimate domains. A three-tier classification scheme was proposed for this system. The first level involved the use of an expert system to detect fast-flux domain queries. The second level involved the use of decision-tree classifiers. The last level involved the use of Naive Bayesian classifiers that would use the statistical knowledge gained from previous fast-flux domains (Stalmans and Irwin, 2011). This last level allowed the system to learn to improve the accuracy in identifying botnets. Overall, the use of the three-tier approach is aimed at improving the accuracy of the predictions and classifications.

2.5 The Role of ISPs

Recent studies, e.g. by Van Eeten et al. (2010), have focused on Internet Service Providers as one of the most important control points for protection of botnets. Three reasons can be distinguished for that. First of all, ISPs are pivotal control point for machines that are already infected. There has been hardly any evidence and comparison between the amount of infected machines that are included in the network of ISP and corporate networks, application service providers and hosting providers. Secondly, there is an assumption that ISPs control a large part of the problem. Here, the focus should not be on legitimate ISPs but rather on the group of "rogue" ISPs—those who are connected with criminal activity. Such rogue ISPs exist within the network of legitimate ISPs and are difficult to detect and identify. From such perspective, legitimate ISPs play the role of control points.

Thirdly, ISPs have solid financial incentive that encourages them to increase their efforts. However, if security (e.g. by quarantining infected customers) is important for ISPs botnets have not yet received significant attention. Presumably, this might be due to the hidden nature of a botnet and its effects (Van Eeten et al., 2010). Therefore, in order for ISPs to successfully mitigate botnet activity, there is a constant need to learn basic features of botnets.

In the initial stage of botnet mitigation ISPs should focus on detection. Livingood et al. (2012) claim that "ISP must first identify that an Internet user [...] is determined to be infected, or likely to have been infected with a bot". On the one hand, ISPs have to use methods that protect privacy-relevant data. On the other hand, legitimate traffic should not be blocked and there should be no disruptions. It can be argued that responsibility for botnet mitigation does not lie on ISPs since they are not the source of it and they would have to take significant costs to make their users protected from potential and existing threats. Furthermore, ISPs loose huge sums of money as stated by Moore et al. (2009) which forces ISPs to take preventive measures make them engaged in anti-botnet campaigns.

Numerous studies report rapid increase of DDoS attacks in size and frequency. According to Arbor Networks (2012), within the period of 2000 to 2010 ISPs have witnessed a growing size of DDoS attacks from less than 1 Gbps to 100 Gbps. As a matter of fact, current botnets are most frequently used for DDoS attacks (Freiling et al., 2005). The study further indicates that the objective of a botnet-based DDoS attack is to cause damage to the target: “In general, the ulterior motive behind this attack is personal which means block the available resources or degrade the performance of the service which is required by the target machine” (Alomari et al., 2012). Because a function of ISPs is to protect their customers from any unauthorised or illegal activities, botnet DDoS attacks are a problem that ISPs have to deal with. Because of the size of botnet-based DDoS attacks (many reaching over 100 Gbps), the issue has gone beyond the scope of one ISP and has been put under social and governmental scrutiny. Botnet-based DDoS will use huge amounts of resources that the ISP has or can take the infrastructure of target ISP out of service.

In addition, by allowing the growth of botnets inside their network ISPs will be seen as unreliable which will significantly damage their reputation. In their empirical study on spam and botnets, Van Eeten et al. (2010, p. 46) claim “because around 80-90% of all spam is issued by botnets, the origin of a spam message is very likely to indicate the presence of an infected machine”. Thus, neglecting the infected computers in their own internal structure, ISPs not only do not eradicate the problem but rather allow it to grow. Ultimately, users of a particular ISP will start receiving constant and regular spam which undermines the professional reputation and reliability of an ISP (Spamhaus, 2014).

2.6 Information Security Risk Analysis Frameworks

Although several different frameworks for information security risk management (ISRM) exist that support a structured risk analysis, Fenz and Ekelhart (2010) conclude that the major problems of ISRM in general is its inability to determine exact values for parameters as likelihood, efficiency of controls or business impact, independent of the applied methodology. Reason for this is the variety of dependencies of certain threats from different parameters and circumstances. Despite of this, Fenz and Ekelhart (2010) state that ISRM frameworks are still able to produce at least certain credible results based on this initial situation of uncertainty. However, the authors also point out that this fact leads to an inherent and often underestimated risk of ISRM frameworks: Organisations applying such frameworks and assessing risks tend to implicitly trust the so gained results regarding their credibility, ignoring the still existing uncertainty of the input data. Still, methodical and structured assessing of risks based on a profound framework support organisations to find clarity in their risks and to understand which possible security controls are adequate, required and value-adding in order to mitigate the overall risk situation.

Several frameworks for methodical information security risk management exist, including NIST SP 800-30 (NIST, 2011), CRAMM (Farquhar, 1991), Octave (Alberts et al., 2003) and ISO 27005 (ISO/IEC, 2011) which were, among others, compared by Fenz and Ekelhart (2010). Although these risk frameworks are widely accepted, Ekelhart et al. (2009) criticise their complexity and the requirement of deep expert knowledge of IT security in general and the respective organisation to successfully apply such methodologies. This is also the reason why many organisations tend to fall back on best practice guidances and international standards. However, the problem with these documents is that applying them on a certain organisation and adequately mapping processes and technologies still requires expertise and specialised knowledge. Without that, results may not be sufficiently sound and credible or, in worst case, the organisation may fail in implementing the ISRM overall.

Ekelhart et al. (2009) generally criticise information security standards like the ISO 27001 series regarding their highly abstract, impractical implementation requirements. The authors state that such standards are too unspecific and lack a certain practicability. On the contrary, Everett (2011) argues that especially the ISO 27005 is flexible because of this abstraction and contains several practical appendices with example lists of threats that can significantly support an organisation in applying this risk management methodology.

To summarise, the study of Fenz and Ekelhart (2010) comes to the conclusion that it is possible to differentiate the existing ISRM frameworks into several phases with tasks that can be mapped towards each other. Based on this, an organisation may decide to apply different methods for different phases of the overall risk management, because there is no single "best" methodology. Each organisation has to decide on a framework, or multiple frameworks, based on its own requirements, organisation culture and circumstances.

Chapter 3

Methodology

This chapter describes the methodical approach of how the work has been carried out. To achieve the objectives of this work, a comprehensive risk-based analysis of the botnet issues in an ISP environment has been conducted. An international standard for information security risk management serves as guidance to define the methodology.

3.1 Understanding the Problem

As necessary preparatory work, it is required to understand botnets as an issue for ISPs. For this, a fundamental description of relevant botnet mechanisms and concepts is required, including communication models, potential vulnerabilities and evasive techniques to prevent shutdown. This initial problem description also has to cover a consideration of motives of botnet operations and of the purposes for which botnets are used.

Without this basic understanding of the problem, a well-founded and conclusive risk assessment cannot be performed and therefore, reliable results are prevented.

3.2 Risk Assessment Approach

This thesis adopts the risk assessment approach of the international standard ISO/IEC 27005:2011, published by ISO/IEC (2011), and applies it in parts to an ISP environment facing botnet threats. Despite the criticised high level of abstraction (see discussion in section 2.6), it was decided to use this methodology because of its generic approach and flexibility. From this, the possibility results to apply it on arbitrary environments, including such a specific environment like the chosen ISP environment with botnet threats. More specialised methods would potentially suffer from a reduced adaptability and problems with applying them onto the given subject may result. In addition, the author of this work has substantial and positive practical experience with both the ISO 27000 series in general and the ISO 27005 in particular, however, not so far in using it in this specific environment.

The ISO/IEC 27005:2011 standard belongs to the *ISO 27000 series* of international standards describing aspects, structure and requirements of information security management and an *Information security management system* (ISMS) in particular.

The process steps highlighted in figure 3.1 are applied, namely *Context Establishment*, *Risk Identification*, *Risk Analysis* and *Risk Evaluation*. Any exceeding application—or even an exhaustive implementation of the whole standard—is beyond the scope of this work.

In general, this work tries to distinguish between *threat*, *vulnerability* and *risk* in conformance with ISO/IEC 27005:2011: A threat could potentially harm something like an asset (e.g. a system or a business process) and can be both accidental or intentional. Vulnerabilities are either intrinsic or extrinsic and can result e.g. from human error or from lack of control mechanisms. Finally, a risk is often associated with uncertainty and arises when a threat has the potential to exploit vulnerabilities and thereby causing harm. Therefore, an approach to reduce risk

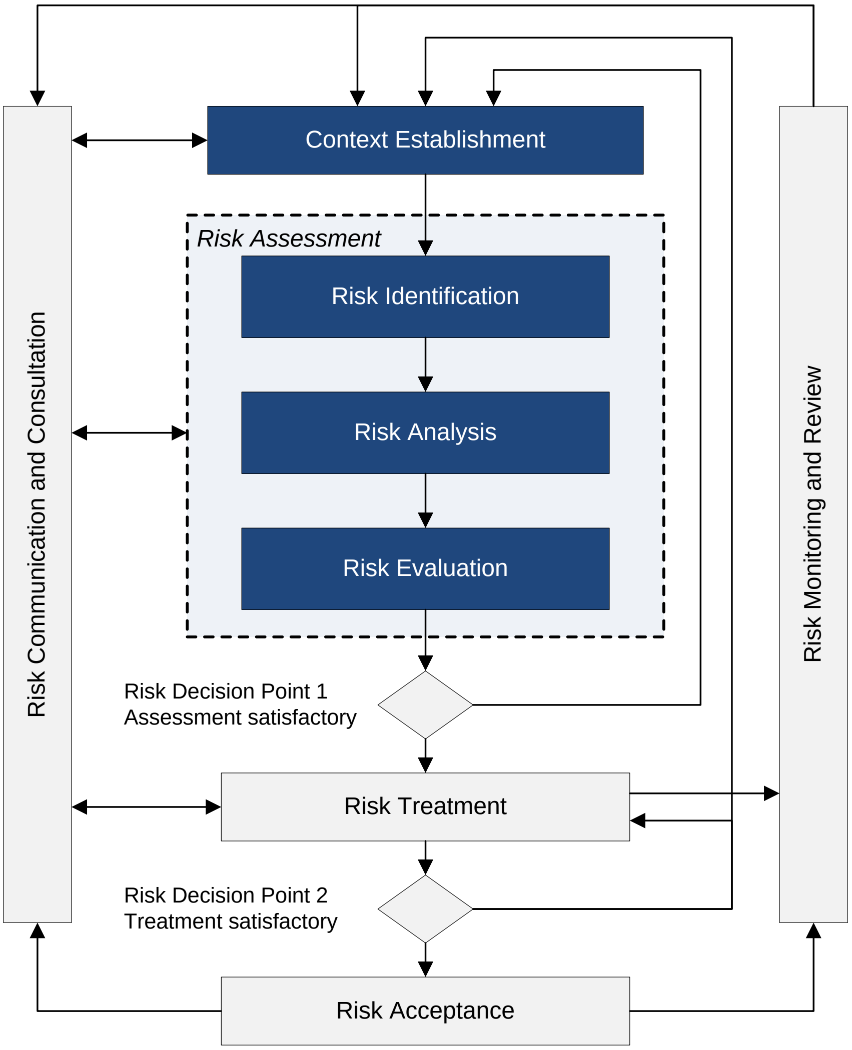


FIGURE 3.1: Risk management process of ISO/IEC 27005:2011 and highlighted its adapted process steps for this work (ISO/IEC, 2011)

can be to either lower or reduce the threat, to reduce or even close the vulnerability, or a combination of both.

3.2.1 Context Establishment

The initial step *Context Establishment* is applied to determine the specifics of botnets and to describe the associated requirements of the ISP environment; this is described in sections 4.1 to 4.3 by discussing significant botnet attributes, the motivation and purpose of botnets as well as the specifics and requirements of ISP environments.

3.2.2 Risk Identification

ISO/IEC (2011) defines *Risk Identification* as a “process of finding, recognising and describing risks” which also includes finding and understanding sources of such risks. This process step is covered in section 4.4.

3.2.3 Risk Analysis

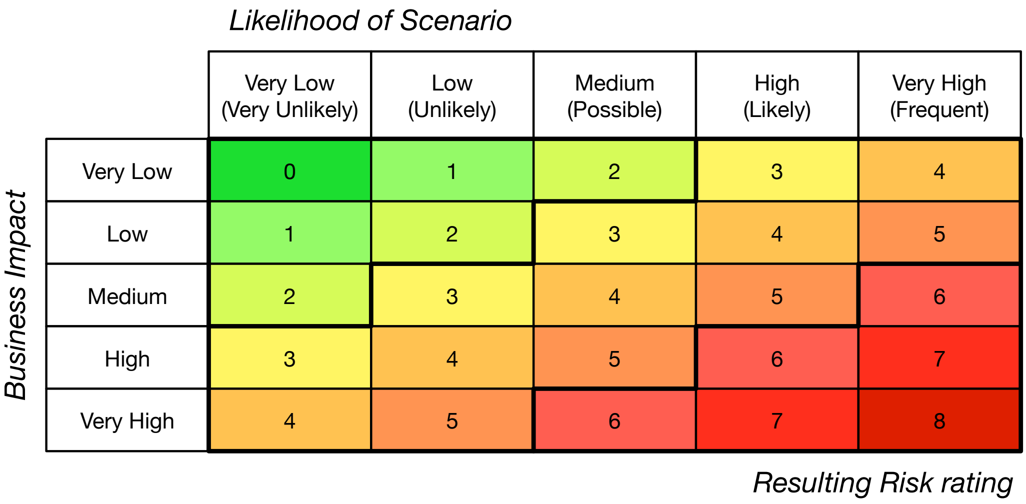
After those preconditions are set, a detailed discussion is then performed in section 4.5 as part of the *Risk Analysis*. It aims at the comprehension of these risks in order to determine a certain level of risk.

3.2.4 Risk Evaluation

Finally, during *Risk Evaluation* in section 4.6 the analysed risks are methodically rated in order to determine if—and to which extent—the risk are significant and require treatment. Based on this structured approach, measures for risk treatment can be derived and implemented. To prepare the subsequent *Risk Treatment* of the risk management process, measures to mitigate botnet risks are discussed in chapter 5.

The evaluation of risks can either be performed by qualitative or quantitative means. For this work, a qualitative approach has been used. As suggested by ISO/IEC (2011, appendix E.2), the matrix shown in figure 3.2 has been used to determine the certain levels of risk by considering the likelihood of a scenario which is mapped against the potential business impact.

The *Risk rating* for a certain risk results from the combination of likelihood and impact rating. The aforementioned risk matrix assigns the highest risk ratings to risks with both high likelihood and high impact, while combinations of high impact but only low likelihood (or *vice versa*) result in reduced risk ratings. If both criteria are low, the resulting risk rating is low too.



Likelihood of Scenario

Business Impact

	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Very Low	0	1	2	3	4
Low	1	2	3	4	5
Medium	2	3	4	5	6
High	3	4	5	6	7
Very High	4	5	6	7	8

Resulting Risk rating

FIGURE 3.2: Risk evaluation matrix with likelihood and impact, based on ISO/IEC (2011, appendix E.2)

Based on the resulting levels of risk, required activities can be prioritised—high risk ratings require high attention and therefore a high treatment priority, while lower rated risks can be treated less prioritised. This approach allows a well-founded decision-making process for the planning of risk treatment and the allocation of further resources and activities.

Chapter 4

Analysis and Results

This chapter describes the analysis results of the risk assessment which were derived according to the methodical approach laid out in the previous chapter. It starts with a discussion of botnet features relevant for the analysed environment and continues with the motivation of botmasters to operate botnets and for what they are typically used. Then, specific characteristics of ISP environments as well as limitations related to botnets are identified. After a comprehensive view on botnet threats for ISPs, the identified factors are analysed and a risk catalogue is derived. Those risks are then evaluated and discussed in order to work out which risks are most threatening for ISPs.

4.1 Significant Botnet Attributes

The controlling entity, the *command & control* (C&C) infrastructure, is under the sole control of the botmaster who manages all of the connected bots. Because of this, robustness, scalability and stability of the botnet substantially depend on this infrastructure. Generally, centralised and decentralised models can be distinguished. They differ in the communication concept and how commands propagate through the botnet.

Bots of a botnet with a centralised architecture connect to a central command entity, consisting of one or several servers (see figure 4.1). The botmaster interacts with this central entity by triggering commands in order to control and query all connected bots (i.e. *active* bots) simultaneously. By this, the botmaster receives immediate feedback and low reaction times of the botnet, because he is able to monitor the state of bots and the botnet as a whole nearly in real-time.

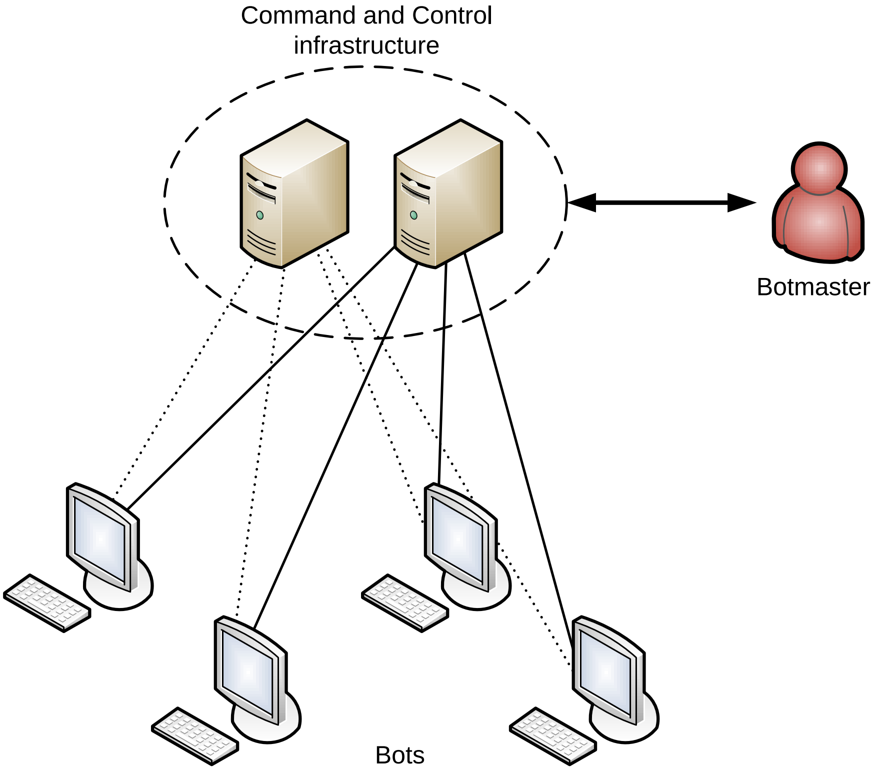


Figure 4.1: Centralised botnet communication model

Larger botnets which follow the centralised architecture may also have a hierarchical, multi-tier distribution of C&C servers. This has advantages both for load distribution and robustness against third party shutdown, but also allows the separation of different server tasks. One example of such a C&C architecture is MegaD, as described by Cho et al. (2010) in detail.

Especially because of this centralisation, the C&C servers pose a major weak point for a botnet shutdown (or *takedown*), as stated by Antonakakis et al. (2012). If these servers are taken offline or shutdown otherwise, the associated botnet is effectively "dead". This is the reason why botnet developers came up with several strategies to improve botnet resilience. Examples for such techniques are *Fast-Flux Service Networks* (FFSN) and *Domain Generated Algorithms* (DGA) which are both based on the Domain Name System (DNS) and will be explained later.

In contrast, the decentralised architecture follows a P2P communication model, which can be seen in figure 4.2. Here, bots are in contact with one or several peers (i.e. other bots) and forward commands to each other. There is no hierarchically superior entity in this concept. The botmaster injects commands from any point within the P2P network which makes him very hard to locate. Those commands are then relayed from bot to bot and so are incrementally propagated through the botnet. This communication model is beneficial regarding robustness to withstand counter-measures. On the downside, the botmaster has to accept slower reaction times of the botnet and possibly a lack of monitoring options (Plohmann et al., 2011, sect. 1.2).

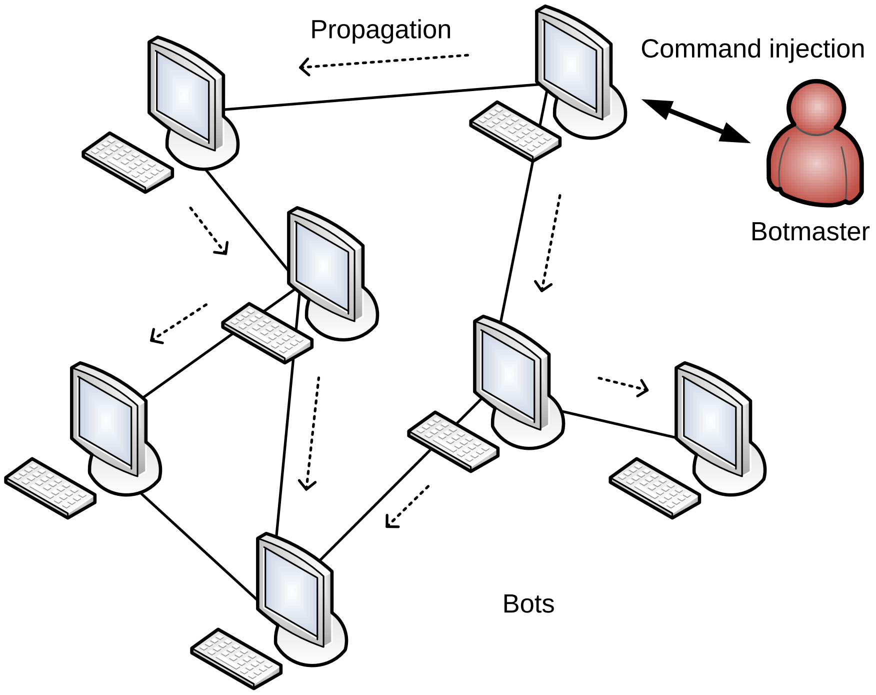


Figure 4.2: Decentralised botnet communication model

When botnets emerged initially, mainly existing and established point-to-multi-point protocols for distributed communication were used, for example IRC and then HTTP too. Meanwhile, botnets have evolved and use more and more customised or proprietary protocols which increasingly implement cryptographic routines, as stated by Plohmann et al. (2011, sect. 1.2). This development complicates their network-based identification and shutdown significantly.

Mainly for the centralised architecture (and less but still for decentralised architecture too) the DNS plays an essential role for the establishment of and the communication within a botnet. By using domain names instead of IP addresses directly in the malware in order to establish a connection to the C&C entity, a level of abstraction is added. It is not sufficient any more to simply blacklist the IP address of the C&C server to shut down the botnet. With DNS abstraction, the botmaster could easily change the name resolution to another IP where an additional C&C server is operated. If, however, the corresponding domain itself is shut down by the registrar authority, bots are effectively cut off from their C&C entity as no successful name resolution can be performed (Antonakakis et al., 2012, chap. 1).

Two mechanisms to cope with this vulnerability—at least one from a botmaster's perspective—are Fast-Flux Service Networks and Domain Generation Algorithms. They are discussed in detail by Holz et al. (2008) and Antonakakis et al. (2012), respectively.

FFSN adapt techniques like round-robin DNS, low *time to live* (TTL) of records and dynamically generated DNS responses which are commonly used by content delivery networks (CDN). They use the bots as relay proxies and rapidly change the relations in order to implement a resilient overlay network. Consecutive DNS requests can still be answered even if single IP addresses are blocked and therefore, the C&C infrastructure stays online (Holz et al., 2008, sect. 2.3).

The idea behind DGA is to use domains for only a short amount of time and to generate new pseudo-random domains for C&C communication dynamically. For this approach it is crucial that the generated domain names cannot be determined beforehand by a third party. The botmaster knows the algorithm and its random seed in order to register upcoming domains. Even if single C&C domains are taken down, the bots reconnect to its C&C entity after the following cycle (Antonakakis et al., 2012).

Overall, it can be concluded that botnets employ sophisticated techniques to avoid both detection and counter-measures. They severely reduce the chance of success of ISPs to implement generic counter-measures. Also, simple measures like blacklisting of C&C IP addresses have only short-time or no effects. Even highly customised solutions against a certain botnet may be ineffective due to rapidly adapting mechanisms like the aforementioned.

4.2 Motivation and Purpose of Botnets

To understand the risks for an ISP which result from botnets, both the typical purpose of botnets and the motivation of botmasters need to be discussed in detail.

Plohmann et al. (2011, sect. 1.2) mention financial gains as the leading motive for operating a botnet. Often, botnets are simply another tool to commit "traditional" criminal offences like fraud, larceny or extortion. Apart from this, political or military interests may be other motives.

Based on these motives, different possible operational scenarios can be found for botnets. Important use cases are large-volume delivery of spam emails (including *scam mails*, *UBE*[2], *UCE*[3] and *phishing emails*), click fraud of online advertisement as well as conducting large scale DDoS attacks. Financial earnings can be generated both directly by operating the botnet (e.g. from manipulating advertising revenues or from demanding ransom in order to end DDoS attacks) and indirectly by hiring botnet resources or services to third parties.

Another significant use case of botnets are theft of sensitive information (e.g. credit card details, login data) or identity theft using sniffing or key logging techniques. Also, botnets can be used for file hosting of illegal material (e.g. pirated software,

[2] UBE: unsolicited bulk email

[3] UCE: unsolicited commercial email

child pornography). The spread of cryptographic technologies makes so-called *resource mining* especially attractive for botmasters, as the available CPU and memory resources of the participating bots can be misused for their own purposes, e.g. by performing brute force attacks on encryption; or by large-scale computation of Bitcoins. Additionally, a botnet can be used to obfuscate an attacker's activities and geographic location in order to avoid criminal prosecution.

Based on the motivation and the use cases of botnets, Plohmann et al. (2011, sect. 5.2) conclude that the distribution of botnets depends on several factors: Simplicity and cost of propagation (i.e. infecting additional systems) is crucial, so is the potential financial gain by operating the botnet. Another factor is the probability and potential severity of impending legal consequences.

All these factors are key leverage points to fight botnets. From an ISP perspective and considering the possible sphere of influence, however, the focus is on technical countermeasures. Coping with botnets can be approached from two sides: First, an ISP can implement measures targeting the ease of botnet propagation and to reduce their size by lowering the amount of customer systems participating in botnets. And second, measures to reduce the impact of malicious botnet activities on the ISP infrastructure can be implemented.

To decide upon adequate and reasonable measures, an ISP needs a risk-oriented basis of decision-making which will be further discussed in the next section.

4.3 Specifics and Requirements of an ISP Environment

This section describes specifics, requirements and limiting factors in order to establish the context as required by ISO/IEC (2011, chap. 7), as part of this work specifically for an ISP environment.

As already stated in section 2.5, the empirical study of Van Eeten et al. (2010) justify the reason to focus on ISPs regarding botnets: They represent critical control points because large amounts of Internet participants rely on the connection services of an ISP and therefore, large amounts of infected hosts reside within the ISP networks. Plohmann et al. (2011, sect. 5.3.2) also agree that due to the unique position to control all of its customers' network traffic, ISPs are able to mitigate the botnet issue.

However, as these authors also point out, privacy laws in different legislations protect ISP customers with regards to network traffic inspection and significantly limit the possible measures. Hence, a thorough analysis of applicable law is required and discussed in section 4.5.

Besides legal issues, other limiting factors or requirements exist for an ISP environment. An ISP with its technical infrastructure differs fundamentally from a corporate environment: Usually, a regular company has its communication endpoints (i.e. the computers) under its own control. That means—related to malware in general and botnets in particular—that a regular company can implement counter-measures on these systems. This may include the installation of malware scan software and a central monitoring of such results. In contrast, an ISP does not have such possibilities, because it does not exercise control over its customers' systems. Therefore, the only option is to implement measures based on network traffic information, but that may hold other challenges.

One substantial question an ISP has to answer is if it is contractually acceptable to implement any measures that have impact on the customer's Internet connectivity. On the one hand, network traffic inspection is more of a legal issue. On the other hand, any subsequently initiated active interference—or any preventative intervention of traffic, e.g. port- or IP-based blocking—can be an infringement of the service contract if the ISP has not ensured the rights to do so beforehand.

Irrespective of issues regarding the feasibility, the question remains unanswered if the ISP holds the responsibility to take actions against botnets at all, especially if customers' systems are infected. This question is independent of the botnet-induced risks for the infrastructure and the services of an ISP, as these and the resulting motivation for counter-measures are further discussed in section 4.4 below. While there may be legal obligations in some countries to do so, it can be seen as more of a moral obligation due to its "critical control point" role to take actions against botnets and botnet-infected customer systems. Additionally, ISPs also act in self-interest when botnets are successfully fought, as they are a major issue for all participants of the Internet economic system. Poor habits regarding botnets can sustainably harm the reputation of an ISP, either in the provider community or in the eyes of customers.

Another ISP requirement is scalability and performance. As opposed to regular companies, an ISP's core competence is delivery of network connectivity. Therefore, already small to mid-sized ISPs have to handle multi-Gigabit Internet bandwidths nowadays. Depending on the customer and network structure, bandwidth rates in the core backbone may be even a multiple of this.

If anti-botnet measures are only implemented for traffic coming into or leaving the ISP network (*inter-AS*, see section 4.4.1), a solution has to cope with the bandwidth coming from and going to Internet upstream partners. Such bandwidth could vary between a few Gigabits up to several hundreds of Gigabits per second. Performance demands will be even higher if *intra-AS* traffic is also in the scope of anti-botnet measures. A suitable product has to be scalable in different levels to keep up with growing bandwidth demands.

4.4 Threat Model for Botnets from an ISP Perspective

Botnets and botnet-induced activities pose severe risks for an ISP and its infrastructure. To make well-founded investment decisions and to follow a strategic approach, an ISP has to know which risks result from botnets for business operations. Therefore, this section discusses threats and risks which arise from botnets.

From an ISP's viewpoint, the operational scenarios *high-volume spam delivery* and *DDoS attacks* are by far the most relevant or potentially most threatening, because these scenarios can have a significant impact on the business operations and service delivery of the ISP. Further on, these scenarios will be generally termed as *botnet activities*. Other botnet use cases like *click fraud* or *identity theft* are of course serious issues but mainly for the customer and not for the ISP, because the ISP is not concerned of or not responsible for the consequences (at least as long as login data of ISP services is not affected) or simply not in the position to mitigate the issues. Therefore, when discussing botnet risks those threats are in focus which result from high-volume spam delivery and DDoS attacks.

4.4.1 Differentiation A: Location of Source and Destination

Consideration of botnet threats can be performed from different viewpoints. One possible approach is to differentiate between source and destination (i.e. target) of botnet activities. Generally from an ISP perspective, the four cases illustrated in figure 4.3 can be distinguished: Either the source of botnet activities (i.e. the bots) are located within or outside the ISP network[4]. Besides, the destination or target of the activities can also reside within or outside the ISP network. Of the resulting four cases, the case with an external source and an external target is not relevant for this work.

For the three remaining cases, it has been reflected which possible impact each case could have and which differences would remain. The case with both internal

[4] An ISP network typically consists of several IP ranges and forms a so called *autonomous system* (AS), identified by the unique *AS number* (ASN). Regular ISPs consist of a single AS, but large, global ISPs (so called *Tier 1 providers*) or other large corporations may consist of several AS. The global compound of interconnected autonomous systems forms the Internet.

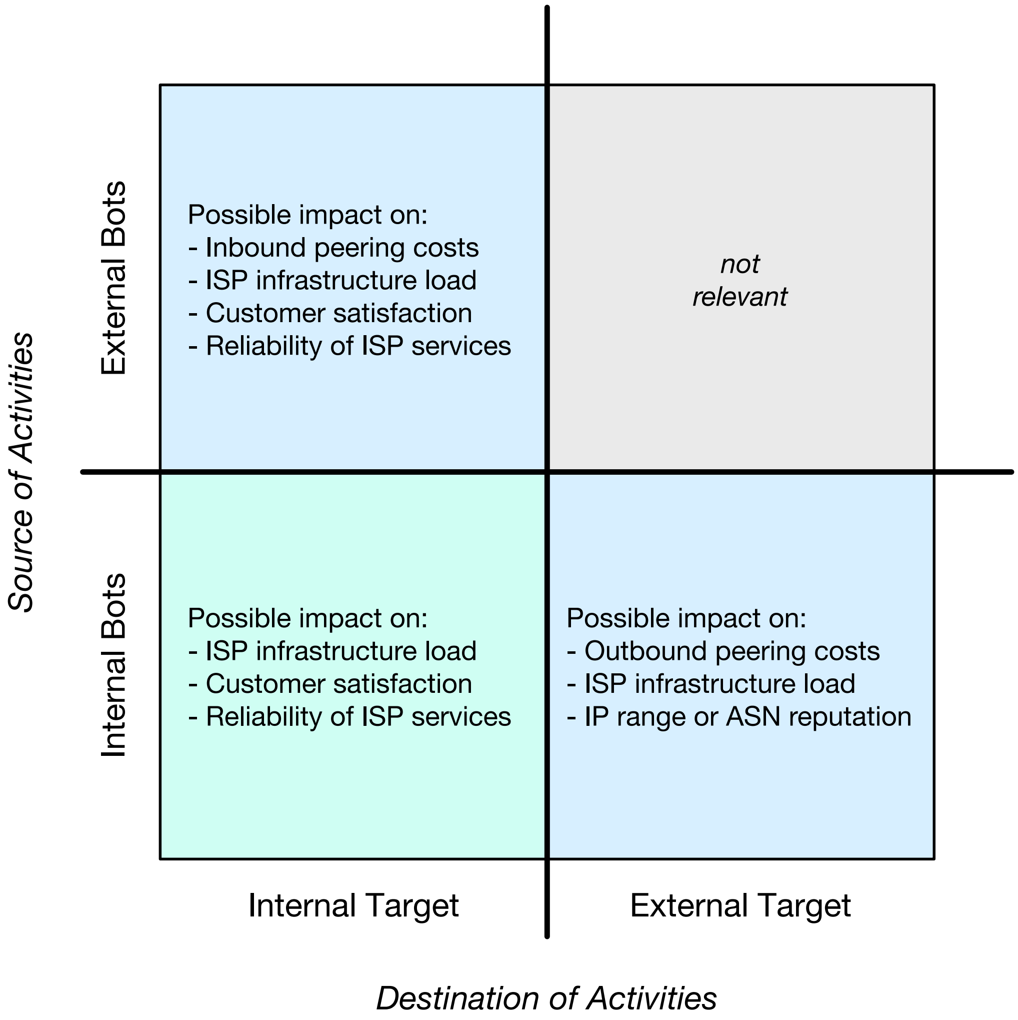


Figure 4.3: Differentiation A – Internal and external participants

source and target will be declared as *intra-AS* as part of this work, while the two cases where the ISP network border is crossed will be called *cross-AS* or *inter-AS*.

External Bots – Internal Target

Especially for DDoS attacks, but for spam activities too, the inbound traffic from other AS would increase. This means, depending on the peering structure of the ISP and its traffic charging, that inbound peering costs would increase too.

The load on ISP infrastructure, e.g. peering routers, core routers and central ISP services like DNS or email infrastructure, would be elevated. Depending on the type and the amount of botnet activities this could vary from beyond noticeable to major decrease in service quality. In extreme cases or if the sizing of infrastructure is inadequate, a total loss of services during the attack is possible.

As a result of service impairment or disruption, customer satisfaction could decrease. The extent would depend on the severity of interference and the amount of affected customers. Overall, the reliability of ISP services could decrease and violation of service level agreements could be the consequence. Such a violation could then result in contractual penalties.

Internal Bots – External Target

In contrast to the first case, now network traffic would mainly flow out of the ISP network. Again, depending on the peering infrastructure and the charging of traffic, an increase in outgoing peering costs would be the consequence.

Similarly, the load on ISP infrastructure would depend on the nature of the activities, but again, minor to major service impact could be the result.

Also contrary to the first case, ISP customers would probably not be affected directly. However, as other systems are attacked from within the ISP AS, other ISPs may feel compelled to sanction the origin of attack. This could lead to the situation that IP ranges are blacklisted by other ISPs because of outgoing attacks, leading to poor ISP reputation. On the one hand, this may have adverse impact on legitimate traffic, e.g. emails are no longer delivered to or from certain destinations because of such blacklisting. If customers are affected of this, customer satisfaction declines and customer loyalty suffers. On the other hand, a bad ISP reputation may also complicate interconnection agreements with other ISPs and therefore may result in a worse peering situation. This, again, may lead to reduced service quality and in the end, lower customer satisfaction and possibly a violation of service level agreements.

Both situations require additional resources and effort of the ISP personnel in order to amend reputation and to initiate removal of blacklist entries.

Internal Bots – Internal Target

Finally, the third case does not fundamentally differ from the first case, where external bots attack internal targets. Of course, peering costs are not affected in this case, but increased load on ISP infrastructure is still a likely result. Similarly, both customer satisfaction and reliability of ISP services may suffer in this scenario with the already mentioned effects on service level agreements.

4.4.2 Differentiation B: Types of Internal Targets

Another possible approach to describe threats resulting from botnets is to further divide the *internal target* of Differentiation A, as shown in figure 4.4. In this case, the threats depend on the nature of the internal target and are independent of the source of botnet attacks, whether from internal or external bots.

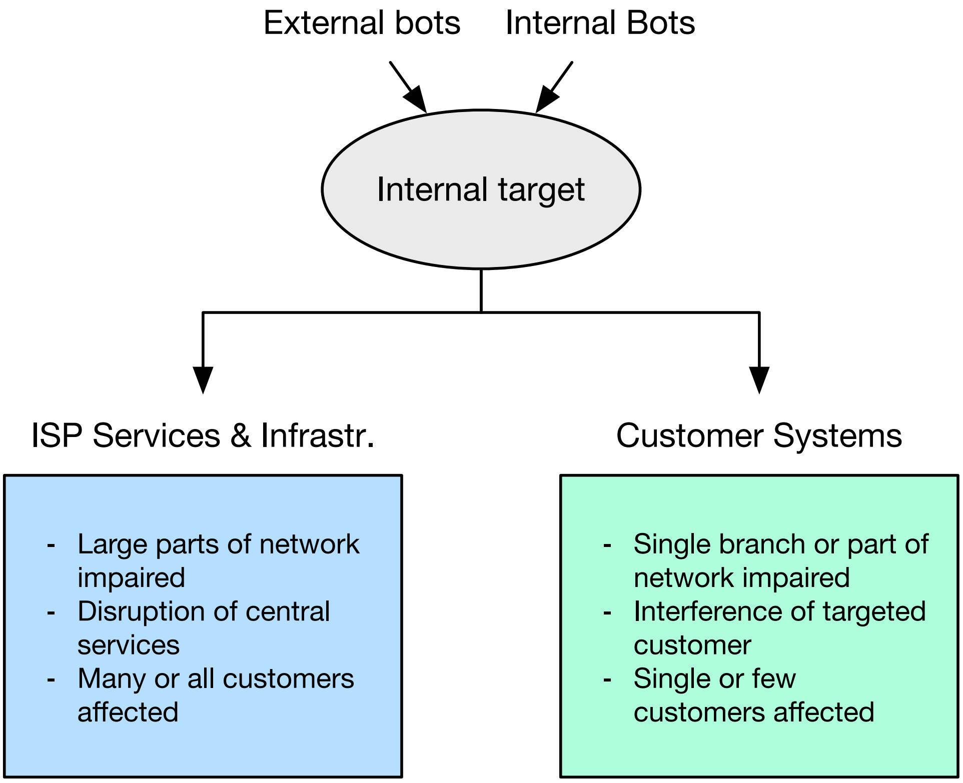

External bots
Internal Bots
Internal target
ISP Services & Infrastr.
Customer Systems
- Large parts of network impaired
- Disruption of central services
- Many or all customers affected
- Single branch or part of network impaired
- Interference of targeted customer
- Single or few customers affected

Figure 4.4: Differentiation B – Possible internal targets

Target: ISP Services and Infrastructure

The first case is that the botnet activities target services or infrastructure operated by the ISP itself that are vital for service delivery. Examples for this case would be: Large spam volumes are delivered to the ISP's email servers; or a DDoS attack is performed directly against ISP systems (e.g. backbone routers, central DNS servers or AFTR[5] gateways).

When considering this scenario, the following threats come up: First of all, depending on the type of attack, large traffic volumes would hit the target. If the botnet is spread across different AS and several countries, it is likely that traffic would enter the ISP network via multiple upstream interconnections. Subsequently, if the attacking botnet is large enough (i.e. the performed attack is strong enough, respectively), the attack would increase load on—and more or less impair—large parts of the ISP network.

In addition, the impact on the targeted system or service would depend on its resilience and maximum load capacity and if any counter-measures are in place. If the attack exploits an existing software vulnerability which leads to a denial-of-service situation (e.g. due to hard reset, freeze or other crash of the component), an immediate service disruption could happen. Alternatively, if the attack simply floods the target with high volumes of requests, the impact could be limited to reduced service quality.

Overall, this scenario would lead to a situation where many or all ISP customers would be affected. Depending on the attacked service or infrastructure, major impact on network connectivity could result which would lead to decrease in customer satisfaction. For business customers, service level agreements could be violated, possibly resulting in contractual penalties for the ISP.

[5] *Address Family Transition Router*, an IPv4/IPv6 transition gateway for *Dual-Stack Lite* networks.

Target: Customer Systems

The other possible case is that an ISP customer is targeted by a botnet. Depending on the size and complexity of the customer's environment, an example scenario could be: The customers hosts his own web servers, the ISP provides Internet connectivity and these web sites are targeted by a DDoS attack.

As a result of such a situation, the impact both on network load and other customers would be limited to the target itself and topological neighbours. The customer's network connection between CPE[6] and ISP network would be the choke point regarding bandwidth, resulting in loss of connectivity for this customer if flooded with higher bandwidths than allocated. Depending on the overall attack bandwidth and the uplink bandwidth of the ISP access node (e.g. DSLAM[7] or the behind BRAS[8]), other customers on the same network branch could be affected too.

4.5 Analysis of Limiting Factors

It has already been mentioned in section 4.3 that legal issues may arise when implementing network-based measures to fight botnets, but the issue needs further elaboration.

For example, the German privacy and data protection laws are rather strict and, together with the telecommunications law for ISPs, set such a high barrier for legally compliant traffic inspection that it is probably unfeasible to implement any. Other countries have similar restrictions based on the idea of confidentiality of (tele-) communication. Especially the countries of the European Union have such

[6] *Customer Premises Equipment*, the demarcation point of the network connection at the premises of a customer. This modem, switch or router (depending on the connection technology) is connected to the access node on ISP side.

[7] *Digital subscriber line access multiplexer*, a multiplexing OSI layer 2 device to connect multiple subscribers to the ISP transport (or *concentrator*) network.

[8] *Broadband remote access server*, the OSI layer 3 routing device to connect e.g. DSLAMs to the ISP backbone network.

laws based on Directive 95/46/EC (1995) and Directive 2002/58/EC (2002) but implement them differently in national law. Notably, the protection requirements of IP addresses differ significantly, resulting in difficulties when processing network flow data (Plohmann et al., 2011, sect. 3.4).

This means that botnet detection and mitigation products may be unsuitable for operation in countries with strict privacy laws if such products are not specifically designed to comply with applicable national requirements. This in general applies to any detection and mitigation approach, e.g. academically developed methodologies too. Only because a method to detect and mitigate botnet threats has been developed and modelled into a certain product does not automatically mean that it can be legally deployed in an ISP environment. The issue is even worse if commercial botnet detection and mitigation products do not clearly reveal their functional approach e.g. because of business secrets. In order to evaluate the affected communication data and to determine legal implications, the detection and mitigation approach needs to be clearly explained.

Another aspect is that botnet detection products designed for use in regular, non-ISP enterprises may not qualify for ISP operations either. Companies may have other legal rights to inspect network traffic due to employer–employee work relation, labour contracts and labour laws, especially if the corresponding endpoint (i.e. the computer system) belongs to the company. However, such less-tight regulations do not apply to the ISP–customer relation.

To conclude the legal aspects, ISPs have to assess applicable laws thoroughly before implementing any anti-botnet measures on the basis of network traffic inspection or manipulation. This is especially relevant for ISPs operating cross-border or globally because different legislations with varying requirements apply. In some countries, a particularly complex situation may occur if privacy laws conflict with telecommunication regulations if they allow (or even require) activities to safeguard Internet security. The idea behind this is that telecommunication services—and therefore Internet connectivity—are part of a country's critical infrastructure and as a result have to fulfil requirements regarding stability, availability and security (Plohmann et al., 2011, sect. 3.4).

Performance requirements are another potential issue of an ISP-qualified product, as already mentioned in section 4.3. If scalability and throughput are not properly designed, investment risks arise because of future bandwidth growth.

4.6 Risk Evaluation

So far, different threats have been identified and discussed. In this section, they are summarised and evaluated to determine certain risk ratings.

To derive a risk rating, the likelihood of occurrence is estimated for each risk. This is combined with an estimation of potential business impact and, based on the already mentioned risk matrix in section 3.2.4, results in a certain qualitative risk rating. Based on these results, decisions can be made and further activities and required measures can be prioritised.

During risk identification and risk analysis which were discussed in the previous sections, multiple threats and issues were identified and described. To summarise, table 4.1 lists the risks R.1 to R.14 which were derived based on these threats during the risk evaluation. Risks with similar numbers and the suffixes *a* and *b* are considered related, but worth to be treated as individual risks because of possibly deviating likelihood or impact ratings.

This catalogue of risks is now further discussed to explain on which threats they are based and how they were determined:

In general, the risks R.1 through R.4 as well as R.10a and R.10b directly result from botnet attacks on targets within the ISP network, as discussed in section 4.4: Botnet activities generate significant network traffic and therefore have impact on peering costs, general network load and service quality. The impact on infrastructure load can further be distinguished between only partial or complete

Risk category	Risk ID	Risk description
Direct result of botnet activities	R.1	Increased peering/upstream costs due to attack traffic
	R.2a	Infrastructure load and congestion of network (partial)
	R.2b	Infrastructure load and congestion of network (complete)
	R.3	Impact on service quality and performance
	R.4	Total loss of important service(s)
Subsequent effect	R.5	Contractual penalty costs due to SLA violation
	R.6a	Decrease of customer satisfaction (only regular or few customers affected)
	R.6b	Decrease of customer satisfaction (premium or many customers affected)
	R.7a	Loss of customers (only regular or few customers)
	R.7b	Loss of customers (premium or many customers)
	R.8a	Damaged ISP reputation (potential customers)
	R.8b	Damaged ISP reputation (carriers, peering partners)
	R.9	Blacklisting of IP ranges with impact on legitimate traffic
Direct result of botnet activities	R.10a	Impact on customer-operated services (regular customer)
	R.10b	Impact on customer-operated services (premium customer)
Implementation of measures	R.11a	Non-compliance of detection measures (legal or contractual)
	R.11b	Non-compliance of mitigation measures (legal or contractual)
	R.12	Non-compliance due to lack of counter-measures
	R.13	Insufficient performance or scalability of measures
	R.14	Ineffective measures against botnets

Table 4.1: Risk catalogue with derived botnet risks for ISP environments

impairment of the network. If ISP services are targeted, risk R.4 results. However, if customer-operated services are targeted, the risks R.10a and R.10b are the consequences. The distinction of regular and premium customers has been made due to their potentially different impact on business operations—premium customers being key accounts, high volume and/or prestigious clients.

When considering the aforementioned risks, the additional risks R.5 through R.9 result from the subsequent effects of botnet attacks, as already mentioned in section 4.4. On the one hand, impact on service qualities may lead to contractual penalty costs if service level agreements are violated (risk R.5). On the other hand, depending on the extent or magnitude of impact customer satisfaction could suffer which is covered by risks R.6a and R.6b. In extreme cases, customers could thereupon terminate contracts, so risks R.7a and R.7b arise.

Overall, the reputation of the ISP could suffer (risk R.8a) and, as a consequence, business operating results may drop. Apart from the customer side, decreased reputation could also result on the side of carriers and peering partners (risk R.8b) which would interfere with future business relations. As discussed in section 4.4.1, if IP ranges of the ISP are blacklisted by other service or hosting providers, adverse effects on legitimate traffic could follow (e.g. emails are not delivered because they are marked as spam) as stated in risk R.9. In consequence, additional effort is required to resolve such issues.

The complex legal situation of botnet-related traffic inspection has been already discussed in section 4.5. As a consequence, risks R.11a and R.11b of possible non-compliance arise, resulting either by violating laws, regulations or contractual agreements. In addition to this possible non-compliance of actually implemented measures, the non-compliance risk R.12 may also be induced by *not* implementing counter-measures if a certain country legally requires ISPs to do so.

ISP networks operate at significantly high bandwidths, as elaborated in section 4.5. Due to these technically challenging requirements, insufficient performance or lack of scalability of solutions is a certain risk taken into account by R.13. If implemented measures do not scale appropriately to the ISP's increasing demands or, as covered by risk R.14, are not effective or efficient, high costs for additional resources, correction or replacement could negatively affect the operational result. In addition, threats of botnets may also not be treated adequately or, mistakenly, the implemented measures give a false impression of the actual security level.

In order to evaluate these identified risks, the risk matrix defined in section 3.2.4 has been applied to each risk individually. For that, the likelihood and potential business impact has been estimated based on personal professional experience. Additionally, generic assumptions regarding an average ISP environment have been taken into account. The derived results can be seen in table 4.2. However, it has to be noted that likelihood estimations are also influenced by measures which are in place to improve resilience of network, services and processes. Therefore, an average ISP environment was assumed—still, deviations may exist in real scenarios or between different ISPs.

To justify those likelihood and impact estimations, the following additional elaboration is required:

Risk R.1: Likelihood of increase in upstream traffic because of large-scale botnet attacks is considered to be *medium*. However, business impact is *very low* due to marginal costs of peering.

Risks R.2a and R.2b: Due to the relatively wide-spread propagation and frequent attacks of botnets, likelihood for partial network congestions is rated *high*, while business impact is *low*. However, the likelihood for large-scale attacks with major or complete network impairment is *very low*, but when they occur a severe business impact follows, therefore considered as *high*.

Risk R.3: Likelihood of service and performance impact in general is estimated *high*, because of the identical probability of occurrence as risk R.2a. Potential impact on business operations is estimated to be *medium* overall.

Risk R.4: Contrary to risk R.3, the likelihood for a total loss of services is only *low*, but the potential impact would be *very high* due to the major consequences for network service delivery.

Risk ID	Impact	Likelihood	Resulting Risk Rating
R.1	very low	medium	2
R.2a	low	high	4
R.2b	high	very low	3
R.3	medium	high	5
R.4	very high	low	5
R.5	low	low	2
R.6a	very low	medium	2
R.6b	low	medium	3
R.7a	very low	very low	0
R.7b	high	very low	3
R.8a	medium	low	3
R.8b	high	low	4
R.9	high	high	6
R.10a	very low	medium	2
R.10b	low	medium	3
R.11a	very high	medium	6
R.11b	very high	medium	6
R.12	very high	very low	4
R.13	high	medium	5
R.14	medium	medium	4

Table 4.2: Risk evaluation results based on likelihood and impact

Risk R.5: SLA (Service level agreement) violation because of botnet attacks is of *low* likelihood. As contractual penalties are considered to be reasonable compared to business operations, only *low* impact is expected too.

Risks R.6a and R.6b: Both likelihoods for decrease of customer satisfaction are rated as *medium*. However, while impact is considered as *very low* if only regular or few customers are affected, it is estimated at least *low* if premium or many customers are affected.

Risks R.7a and R.7b: Similarly to risks R.6a and R.6b, the likelihood of the risk of loosing customers due to botnet activities is considered equally *very low*.

But while the loss of regular or few customers would have *very low* consequences for overall business, loosing premium or many customers because of botnets would have a *high* impact on the ISP's operational results.

Risks R.8a and R.8b: Both likelihoods for these risks are rated *low*, because anti-botnet measures are neither widely spread on ISP level nor considered as reputation-related by customers *(yet)*. If reputation is damaged from a potential customer's viewpoint, business impact is *medium* because of the highly competitive market. However, if reputation is damaged from a carrier's or peering partner's perspective, business impact is *high*, because it negatively affects peering cooperations, leading to bad AS interconnections.

Risk R.9: Getting blacklisted is of *high* likelihood nowadays due to wide-spread botnet infections of ISP customers. The impact is *high* too, because significant additional effort is required to convince third parties to correct their blacklists.

Risks R.10a and R.10b: Both likelihoods for these risks are rated as *medium*. However, while impact is considered as *very low* if only regular or few customers are affected, it is estimated *low* if premium or many customers are affected.

Risks R.11a and R.11b: Due to the complex legal requirements for detection and mitigation activities, likelihood of non-compliance is rated *medium*. Typically, ISPs are operating in a heavily regulated market and regulatory authorities could sanction non-compliance with severe restrictions (up to interruption of business activities) which would result in *very high* impact on business operations.

Risk R.12: If an ISP is legally obliged to implement counter-measures, non-compliance by not doing so could—similarly to risks R.11a and R.11b—result in sanctions with *very high* impact. However, its likelihood is only *very low*, because typically ISPs are involved (or otherwise notified) if such laws are adopted anyway.

Risk R.13: Typically, ISP environments have enormous bandwidth processing demands and a *medium* likelihood has been estimated that these requirements may not be met by implemented solutions. If this is the case, a significantly *high* impact on business operations is expected because the whole network could be impaired by this and high costs may result to compensate the ineffectiveness.

Risk R.14: Finally, due to the complex and constantly evolving nature of botnets, likelihood of ineffective counter-measures is considered *medium*. Based on the overall botnet threats on ISP environments, the impact by such an ineffectiveness is rated *medium* too.

After applying the defined risk matrix on all identified, analysed and evaluated risks R.1 to R.14, the resulting risk ratings are illustrated in figure 4.5. Especially the top-rated risks, namely risks R.9, R.11a and R.11b with a rating of *6* as well as risks R.3, R.4 and R.13 with a *5* rating, should be high priority risks for every ISP and require considerable attention and effort for risk treatment.

In order to focus on these high priority risks, they are revised in table 4.3.

Risk ID	**Risk description**
R.3	Impact on service quality and performance
R.4	Total loss of important service(s)
R.9	Blacklisting of IP ranges with impact on legitimate traffic
R.11a	Non-compliance of detection measures (legal or contractual)
R.11b	Non-compliance of mitigation measures (legal or contractual)
R.13	Insufficient performance or scalability of measures

Table 4.3: Top-rated risks which require high priority

It has to be noted that the structured and methodical analysis carried out in this chapter did not identify any risks with the highest possible ratings *7* or *8*.

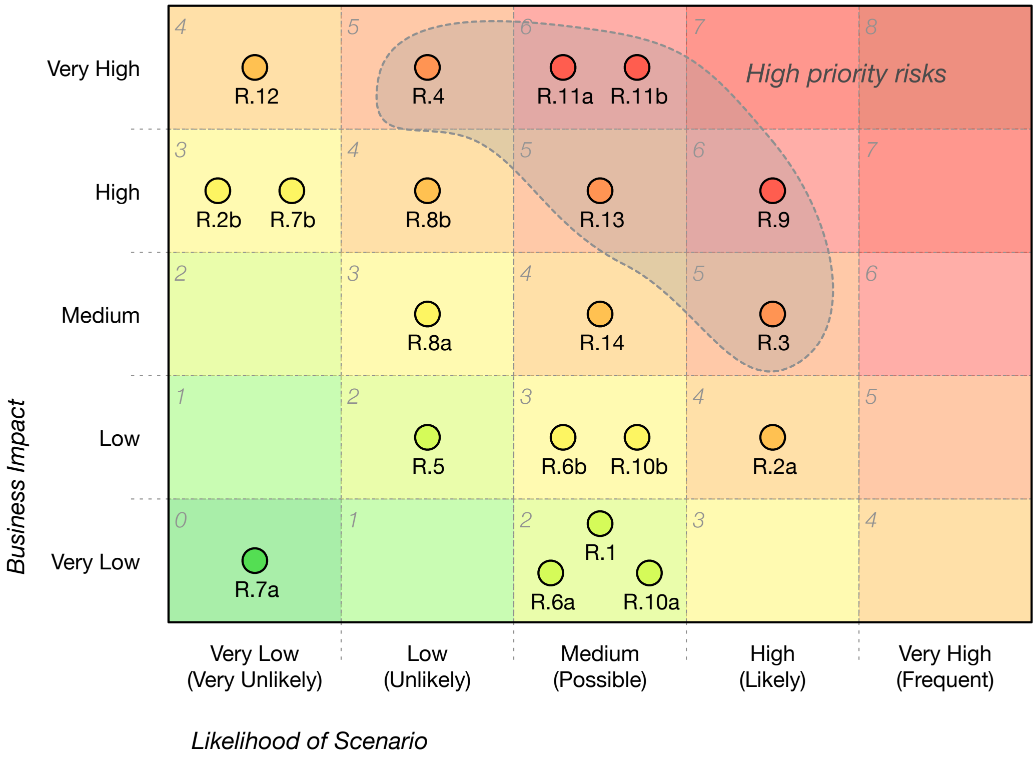


FIGURE 4.5: Overall risk ratings of risks R.1 to R.14

Further discussion of the resulting implications of these risks for ISPs and of possible counter-measures are performed in chapter 5.

Chapter 5

Discussion and Evaluation of Results

This chapter discusses and evaluates the results of the analysis phase in detail. The identified and rated risks are considered both individually and in the wider context by stating implications for ISPs and by drawing conclusions for dealing with botnet risks. After that, the results and applied methods of this thesis are critically evaluated in order to appraise the overall performance and the practical value of this work.

5.1 Discussion of Identified Risks

To discuss the possible mitigation approaches of risks in general and of those identified in particular, it has to be noted that this can either be achieved by reducing its likelihood of occurrence or by lowering the possible impact on business operations. Based on the applied risk matrix (see section 3.2.4), such a reduction automatically leads to a decrease of the risk. Typically, it is easier or more feasible to influence the likelihood of occurrence instead of reducing the business impact. This is because reducing business impact often requires extensive changes of how a company generates profits, how it is positioned on the market or which processes and technologies are incorporated.

Initially, the identified risks in section 4.6 are discussed individually to determine whether and how mitigation is possible. The subsequent section discusses overall implications in a wider context.

The impact of risk R.1 cannot really be reduced. The cost structure of peerings is relatively fixed and cannot be lowered for botnet traffic. The only conceivable approach to reduce the likelihood of this risk would be to reduce the overall attractiveness of the ISP's network for inbound botnet attacks. However, an ISP would hardly change his customer structure to achieve this. Although, implementing anti-DDoS measures and anti-spam filters could reduce the overall success of botnet activities and therefore the possible financial gain of botmasters related to this ISP. To address the likelihood of outbound botnet attacks, an increase in customer awareness regarding malware and botnet threats could be an approach. Additionally, rate or bandwidth limits on network level, blocking of certain network ports[9] or temporary blocking of subscriber lines in case of ongoing, confirmed botnet activities. For the last case, immediate customer notification is required, though.

If an ongoing botnet attack is present, additional actions are required that depend on the actual nature of the attack. One possible action is blocking of source or target of attack traffic on network level. However, if the attack is heavily distributed, source blocking is not feasible any more. In order to protect the overall network or the affected network part, a temporary shutdown of the targeted IP may be required. Typically, this is achieved by so called *blackholing*, i.e. silently discarding traffic on backbone router level by setting a *null route* "to nowhere" for the affected IP. To generally relieve the ISP network, such blackholing should already be performed at incoming peering partners if large attack bandwidths are observed. Thus, attack traffic does not enter the ISP network at all.

[9] e.g. TCP port 25 (SMTP) for outgoing email transfers is not required for end-user lines.

In consequence, anti-DDoS and anti-spam measures also reduce both the likelihood and the impact of the risks R.2a, R.2b, R.3 and R.4. Sufficient reserve capacities of network components and services as well as increased redundancies also help to cope with these risks by reducing the likelihood of occurrence, especially those of risks R.2b and R.4.

Business impact of the risks R.10a and R.10b cannot be influenced as this is in the customer's responsibility. However, the likelihood for customers can be reduced by implementing additional (potentially chargeable) protective services.

If all the risks are reduced that directly result from botnet activities, the likelihoods of occurrence is reduced for the risks R.5 to R.9 as a consequence due to their subsequent nature. After all, the business impact of these risks cannot be lowered by the ISP anyway.

Related to the implementation of measures it can be concluded that the overall likelihoods of the risks R.11a to R.14 can be reduced by significant carefulness and preparation before deciding on measures. For this, the involvement of other departments and experts (e.g. a specialist solicitor for IT and telecommunications) is necessary. Especially the likelihoods for the risks R.13 and R.14 can be significantly reduced by a careful and well-considered selection of measures and products.

5.2 Specifics of the Environment

To fight botnets, an approach is to take steps against the motivating factors as described in section 4.2. However, for an ISP in its position there is only little that can be done which is now further explained.

First of all, the simplicity and cost of propagation can be addressed. To prevent customers from getting infected with botnet malware in the first place, increasing awareness is a promising approach. If systems are already infected, another approach is to limit or block botnet communication—but for this being successful, relevant communication has to be reliably detected first. The major problem is that for an ISP this detection is associated with many obstacles, as will be further discussed below.

The next motivating factor—financial gain by operating the botnet—can be addressed by an ISP from two sides. First, fighting spam in order to reduce the successful delivery of unwanted emails to the customer's mailbox is a way to reduce the financial gain of botmasters. Most probably, an ISP has already implemented some sort of spam filter anyway. The other major use case of botnets are DDoS attacks, possibly combined with extortion to stop such attacks. The financial gain by that can be reduced by increasing the general resilience of the network and services in order to lower the DDoS vulnerability—if a botmaster requires more bandwidth to harm a target, he needs a larger botnet and more resources, therefore the overall effort is higher and his remaining profits decline.

The threats of other use cases of botnets, namely click fraud, identity theft or resource mining, cannot be mitigated by an ISP due to lack of control. Blocking communication in order to bring down C&C traffic can help with these issues too, though.

The third motivating factor is probability and extent of potential severity of legal consequences. An ISP is able to influence this factor by increasing the likelihood of catching botmasters. To achieve this, detection measures can be a feasible approach but suffer from implementation difficulties. However, another approach for an ISP is to connect both with authorities, expert groups and researchers to exchange information about ongoing activities to support and speed up criminal prosecution.

An ISP can come to the decision that it is not in his responsibility to deal with botnet issues. But if he does so, this results in long-term problems that have negative impact on business operations. As analysed in section 4.4, loss of reputation—both on customer-side and carrier-side—leads to poor peerings and customer losses. Not mitigating botnet threats results in major decrease in service quality and availability, further expediting customer churn. Developments of the legal status could result in non-compliance, if the ISP is obliged to take preventive actions to protect his network and his customers. Overall, the ISP will have to bear the negative consequences if the botnet problem is ignored or considered not relevant. Inevitably, botnet activities will continue, so as infected customer systems will exist in the ISP network.

However, the analysis of the specifics and requirements of ISP environments in section 4.3 has shown that one major challenge for an ISP lies in implementing detection measures for botnets. It is only feasible to detect based on network traffic and such activities are potentially under strict regulation which has been shown in section 4.3. Although different detection approaches exist that have been described in chapter 2, some of them may be either critical from a legal perspective, not suitable for an ISP environment (e.g. because of performance requirements) or not generic enough (e.g. because only focused on a certain botnet). To sum up, it is questionable if implementing botnet detection solutions as a preventive measure is practically feasible and/or economically reasonable. Each ISP has to analyse the specific legal situation to be able to make this decision.

In addition to this, the situation is complicated by the fact that botnets are constantly evolving and techniques are improved to avoid detection and countermeasures. Successful detection is significantly hampered as cryptographic protection mechanisms prevail more. If detection of botnets is not possible, their shutdown is effectively prevented too. But also other techniques like FFSN or DGA lead to the fact that counter-measures on network level, e.g. blacklisting of C&C domains or IPs became actually non-effective too. Similarly, by the increasing use of web-based C&C over social media that has been described by Goranin et al. (2012), blocking of such network traffic becomes obsolete—after all, an ISP cannot cut off his customers from Twitter and Facebook without significant resistance.

From this perspective, it is debatable whether an ISP can only reactively perform activities anyway. One major task would be to inform involved customers—an approach that is also emphasised by Plohmann et al. (2011, p. 7) who state that the information flow via the ISP to notify end-users is a useful and effective method. However, the authors also indicate that this results in extra costs for ISPs which therefore require some sort of incentive to bear those costs. Lowering the risks derived in this thesis may be such an incentive, though.

Besides, for this approach to be successful, the ISP also has to have the relevant information present. This means, several communication interfaces have to be established. Points of contact have to be defined, adequately instructed and trained for customer requests and for customer notification. In addition, external requests—either from peering partners, agencies or other concerned parties—have to be channelised and processed in a timely manner.

Traditionally, an ISP operates a so called *abuse mailbox* that can be used to report such kind of malicious activities related to the ISP's AS. This mailbox is listed in the *whois* database on IP range and AS level and most of the time has the email address *abuse@isp-domain* assigned. All parties need to be aware of such points of contact that are ideally presented on the ISP's web site too. Despite that, processes and personnel are also required to handle such reports properly. Botnet-related information needs to be classified and forwarded to the respective security engineers who then can initiate appropriate steps, including verification of information, immediate actions and notification of affected customers with necessary counter-measures (e.g. disinfecting computers, properly securing networks, etc.).

In addition, communication interfaces towards peering partners are necessary to effectively mitigate ongoing DDoS attacks by blackholing IPs at upstreams providers. Defining points of contacts is also useful to cooperate with agencies, law enforcement, expert groups and academic research facilities. On the one hand, such institutions can provide vital information about ongoing trends, developments and attack patterns. On the other hand, if they are able to contact ISPs more quickly to get support and to trigger response actions on ISP side, botnets can be taken down more easily. In the long term, communication interfaces to connect the different stakeholders can significantly support the fight against botnets.

Furthermore, it can be advisable for an ISP to consider proactive actions to fight botnets. Participating in large-scale anti-botnet measures of research or expert groups e.g. by supporting honeypots to gain deeper insights into new botnets can possibly prevent certain threats before they arise in the first place—as long as these activities are legally compliant.

5.3 Evaluation of the Methodical Approach and the Results

The results gained throughout this thesis could clearly disprove the conclusions of both Van Eeten and Bauer (2008) as well as Van Eeten et al. (2010) who state that there exist only very few incentives for ISPs to take actions against malware (so including botnets). The identified and evaluated risks in section 4.6 clearly show that several risks pertain to ISPs which are able to significantly impair or interrupt business operations. By implication, these risks represent *strong* incentives to implement measures against botnets in order to mitigate those business-threatening risks and, based on the applied methodology, this thesis was able to present specific measures to reduce these risks by lowering the likelihood and/or impact. Despite the fact that a similar risk evaluation approach based on the ISO 27005 risk matrix has been used, the risk results of this work are not comparable to those of Elliott (2010). The first reason for this is the different environment, as Elliott (2010) performed the risk evaluation from a public and government perspective. The second reason is that the viewpoint on threats is significantly more abstract compared to the much more detailed approach of this thesis.

The question remains if the risk assessment methodology of ISO/IEC 27005:2011 and how it was applied to the given environment as described in section 3.2 was an adequate approach to achieve the goals of this thesis. Based on the insights during the analysis, compared to practical risk assessment experience and considering the comprehensive and sound results, the author's opinion is that the applied process of ISO/IEC 27005:2011 was a reasonable choice for this work. Although Ekelhart et al. (2009) criticise the complexity and high level of abstraction, for this thesis it became apparent that these characteristics of the standard were beneficial for applying the methodology onto the very specific ISP environment with its unique limitations and requirements.

Especially the initial step of *Context Establishment*—defined in section 3.2.1 and implemented in sections 4.1 to 4.3—supported to define the environment by focusing on the limiting factors and the requirements. Additionally, the differentiation between identification, analysis and evaluation of risks, e.g. by describing a comprehensive threat model of botnets as performed in section 4.4, supported the structured derivation of results and increased overall reliability. Other methodologies which either do not intend such a context definition at all or simply apply generic roles or business models may not have produced similarly profound results. Still, as stated by Fenz and Ekelhart (2010), other frameworks may also be suitable for certain organisations—but those were not covered in this thesis.

However, another criticism of the applied standard could be confirmed during the analysis. Ekelhart et al. (2009) state that risk frameworks are complex and require deep expert knowledge. To estimate likelihoods and business impacts, extensive knowledge of ISP operations and business processes was required. In fact, the overall quality of the resulting risk ratings heavily depend on these estimations. In addition, the gained results have to be critically reviewed before applying them to a certain practical ISP environment, in so far as they have been derived based on generic assumptions without considering any existing controls or counter-measures.

Chapter 6

Conclusions

In conclusion, this thesis was able to meet its overall aim which is, as stated in section 1.2, to perform a methodological risk analysis of botnets for an ISP environment. The derived and discussed results from the structured analysis in sections 4.6 and 5.1 were able to fully answer the initially stated research questions regarding the threats an ISP faces from botnets as well as which requirements and restrictions exist for the detection and mitigation of botnets as ISP. However, the second aim—to enable an ISP to decide on measures to minimise botnet threats for the infrastructure—was only partially met because further assessment of the results regarding their business value would be required to fully achieve that. This final chapter concludes the thesis by discussing the overall achievement of the objectives and by stating limitations and possible future work based on the insights.

6.1 Achievement of Objectives

As initially stated in section 1.2, the following five objectives were defined for this thesis:

1. Perform a literature review by investigating and reviewing relevant literature in the fields of botnets, ISP threats and risk assessment schemes.

2. Decide upon the risk assessment approach and consider the overall methodology that is going to be used.
3. Perform an extensive risk assessment of botnet threats on ISP environments by identifying and evaluating associated risks.
4. Discuss the results from the risk assessment, how these can be mitigated and which recommendations for ISPs result.
5. Evaluate the outcome of the thesis as well as the applied methods and techniques and appraise the contributed value of the results.

These objectives are now individually discussed to show if and how they have been achieved.

6.1.1 Objective 1: Literature Review

This objective was successfully met by chapter 2. A literature review has been performed in the fields of botnets, ISP threats and risk assessment frameworks to discuss relevant work. The investigated research showed that botnets progressively implement sophisticated techniques to avoid detection of C&C communication and to improve robustness against shutdown. This development poses major challenges to implement preventative counter-measures. Recent studies focused on ISPs and identified them as important control points to fight botnets, but did not cover the associated requirements and limiting factors for ISPs to actually implement counter-measures.

In addition, the review of material revealed that some work has been done regarding botnet threats. However, the existing work neither targeted ISP environments nor was thoroughly performed on a detailed level based on a structured risk identification, analysis and evaluation. Although different risk frameworks exist, they share common weaknesses regarding complexity and required skills. Discussed studies showed that the selection of a certain framework is highly dependent on the specific organisation.

6.1.2 Objective 2: Methodology

This objective was successfully addressed in chapter 3 where the risk framework of ISO/IEC 27005:2011 was chosen because of its flexibility and due to existing knowledge and practical experience of the author. The overall methodology of the analysis phase was defined based on selected process steps of the standard in order to support the aims and objectives of the thesis.

The defined methodology consisted of the context establishment to describe the environment, the risk identification to find and describe risks, the risk analysis to discuss those risks in detail and, lastly, the risk evaluation to determine the levels of risk based on a risk evaluation matrix in order to focus on major risks and to allow sound decisions for treatment.

6.1.3 Objective 3: Risk Analysis

This objective was successfully achieved and reported in chapter 4 by applying the defined methodology. The comprehensive results of the analysis were presented by describing relevant botnet attributes and by extensively stating the motivation and purpose of botnets. Subsequently, the ISP environment was examined by identifying specifics and requirements as well as by showing limiting factors regarding botnet detection and mitigation.

Based on a comprehensive threat model of botnets and an analysis of limiting factors for ISPs, the resulting twenty risks of the subject were assessed. After evaluating and justifying the associated likelihoods of occurrence and possible business impacts, the overall risk ratings were derived and the six top-rated risks were highlighted by defining them as high priority risks.

6.1.4 Objective 4: Discussion of Results

This objective was successfully met by chapter 5 which discussed the results from the risk assessment in detail. The identified and evaluated risks were considered both individually and in the wider context. For this, resulting implications for ISPs and conclusions for mitigating botnet risks were discussed. This could be achieved by stating possibilities to either reduce the risk's likelihood of occurrence or to lower the potential business impact of the risk.

Based on the extensive discussion, recommendations for ISP were given. To conclude, both preventative and reactive measures and processes are necessary on ISP side. Implemented anti-DDoS and anti-spam measures are able to mitigate several identified risks, both directly and indirectly. Additionally, extensive communication interfaces to other stakeholders are required to improve information flows. Other risks cannot be mitigated because the factors are outside the ISP's influence. Still, recommendations for counter-measures could be given to address almost all risks.

6.1.5 Objective 5: Evaluation

Finally, this objective was successfully achieved by chapters 5 and 6 where the methodical approach of the analysis as well as the results were critically evaluated. Overall, the methodical approach was believed to be adequate and the applied risk framework of ISO/IEC 27005:2011 to be suitable. The results could clearly show strong incentives for ISPs to act on botnet issues, disproving other existing studies that state there are only few. However, it could be confirmed that the application of risk frameworks is highly complex and requires expert knowledge of IT security, the associated threats and the relevant environment. In summary, the thesis achieved its objectives.

6.2 Limitations and Future Work

This work applied the risk management approach of ISO/IEC 27005:2011 by performing a risk identification, analysis and evaluation based on estimated likelihoods and impacts. However, other risk frameworks may also be suitable to apply them to the given ISP environment and be able to produce adequate results. It is hard to predict if another risk framework would produce comparable or even the same results like those of this work, because any risk framework results also depend on the respective knowledge and experience of the authors. Still, a possible research area may be to perform a similar risk assessment with another risk framework and to compare the results in order to disprove, confirm or expand the gained results of this work.

The major limitation of this work and its results is that they are clearly theoretical without getting applied on a real-world environment to confirm feasibility and adequacy of recommendations. Although this work considers costs during the evaluation of possible business impacts, a subsequent analysis of cost value from business perspective was not performed due to its limited scope. However, as ISP the gained risk results and given recommendations have to be assessed from business perspective before any decisions regarding risk mitigation can be made. Further research in this area is required in order to process the results of this work. Based on such further work, the second aim of this thesis—to enable an ISP to decide on measures to minimise botnet threats for the infrastructure—would also be fully achievable.

Bibliography

Akkaladevi, S. and Katangur, A. K. (2010), 'Defending against botnets', *Journal of Applied Global Research* **3**(7).

Al-Ahmad, W. and Al-Ahmad, A. (2014), Botnets detection using message sniffing, *in* 'The International Conference on Digital Security and Forensics (DigitalSec2014)', The Society of Digital Information and Wireless Communication, pp. 40–45.

Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003), 'Introduction to the octave approach', *Pittsburgh, PA, Carnegie Mellon University* .

Alomari, E., Manickam, S., Gupta, B., Karuppayah, S. and Alfaris, R. (2012), 'Botnet-based Distributed Denial of Service (DDoS) attacks on web servers: Classification and art', *International Journal of Computer Applications* **49**(7), 24–32.

Antonakakis, M., Perdisci, R., Nadji, Y., Vasiloglou II, N., Abu-Nimeh, S., Lee, W. and Dagon, D. (2012), From throw-away traffic to bots: Detecting the rise of DGA-based malware, *in* 'USENIX Security Symposium', pp. 491–506.

Arbor Networks (2012), 'Anatomy of a botnet: How the Arbor security engineering & response team (ASERT) discovers, analyses and mitigates DDoS attacks'.
URL: *http://www.arbornetworks.com/images/documents/White%20Papers%20and%20Research/WP_ASERT_EN.pdf*

Asghari, H. (2010), Botnet mitigation and the role of ISPs: A quantitative study into the role and incentives of Internet Service Providers in combating botnet propagation and activity, PhD thesis, TU Delft, Delft University of Technology.

Aycock, J. (2006), *Computer Viruses and Malware*, Advances in Information Security, Springer.

Bauer, J. M. and Van Eeten, M. J. (2009), 'Cybersecurity: Stakeholder incentives, externalities, and policy options', *Telecommunications Policy* **33**(10), 706–719.

Cho, C. Y., Caballero, J., Grier, C., Paxson, V. and Song, D. (2010), Insights from the inside: A view of botnet management from infiltration, *in* 'USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)'.

Dunham, K. and Melnick, J. (2008), *Malicious bots: an inside look into the cyber-criminal underground of the Internet*, CRC Press.

Ekelhart, A., Fenz, S. and Neubauer, T. (2009), Aurum: A framework for information security risk management, *in* '42nd Hawaii International Conference on System Sciences, 2009 (HICSS'09)', IEEE, pp. 1–10.

Elliott, C. (2010), 'Botnets: To what extent are they a threat to information security?', *Information security technical report* **15**(3), 79–103.

European Parliament and the Council of the European Union (1995), 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', *Official Journal of the European Union* **L 281**, 31–50.

URL: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML*

European Parliament and the Council of the European Union (2002), 'Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic

communications)', *Official Journal of the European Union* **L 201**, 37–47.
URL: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML*

Everett, C. (2011), 'A risky business: Iso 31000 and 27005 unwrapped', *Computer Fraud & Security* **2011**(2), 5–7.

Farquhar, B. (1991), 'One approach to risk assessment', *Computers & Security* **10**(1), 21–23.

Fenz, S. and Ekelhart, A. (2010), 'Verification, validation, and evaluation in information security risk management', *IEEE Security & Privacy* (2), 58–65.

Freiling, F. C., Holz, T. and Wicherski, G. (2005), *Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks*, Springer.

Gassen, J., Gerhards-Padilla, E. and Martini, P. (2013), Botnets: How to fight the ever-growing threat on a technical level, *in* 'Botnets', Springer, pp. 41–97.

Goranin, N., Čenys, A. and Juknius, J. (2012), 'Malicious botnet survivability mechanism evolution forecasting by means of a genetic algorithm', *Science–Future of Lithuania/Mokslas–Lietuvos Ateitis* **4**(1), 13–19.

Holz, T., Gorecki, C., Rieck, K. and Freiling, F. C. (2008), Measuring and detecting Fast-Flux Service Networks, *in* 'NDSS'.

ISO/IEC (2011), Information technology—Security techniques—Information security risk management, ISO/IEC 27005:2011, International Organization for Standardization (ISO) and International Electrotechnical Commision (IEC).

Livingood, J., Mody, N. and O'Reirdan, M. (2012), RFC 6561: Recommendations for the Remediation of Bots in ISP networks, Technical report, Internet Engineering Task Force (IETF).

Moore, T., Clayton, R. and Anderson, R. (2009), 'The economics of online crime', *The Journal of Economic Perspectives* **23**(3), 3–20.

NIST (2011), Guide for conducting risk assessments, Technical Report SP 800-30, Rev. 1, National Institute of Standards & Technology.

Plohmann, D., Gerhards-Padilla, E. and Leder, F. (2011), 'Botnets: Detection, measurement, disinfection & defence', *The European Network and Information Security Agency (ENISA)* .

Spamhaus (2014), 'Spamhaus botnet summary 2014'.
URL: *http://www.spamhaus.org/news/article/720/spamhaus-botnet-summary-2014*

Stalmans, E. and Irwin, B. (2011), A framework for DNS based detection and mitigation of malware infections on a network, *in* 'Information Security South Africa (ISSA), 2011', IEEE, pp. 1–8.

Stinson, E. and Mitchell, J. C. (2008), Towards systematic evaluation of the evadability of bot/botnet detection methods, *in* 'Proceedings of the 2nd USENIX Workshop on Offensive Technologies (WOOT 08)', Vol. 8, pp. 1–9.

Tiirmaa-Klaar, H. (2013), Botnets, cybercrime and national security, *in* 'Botnets', Springer, pp. 1–40.

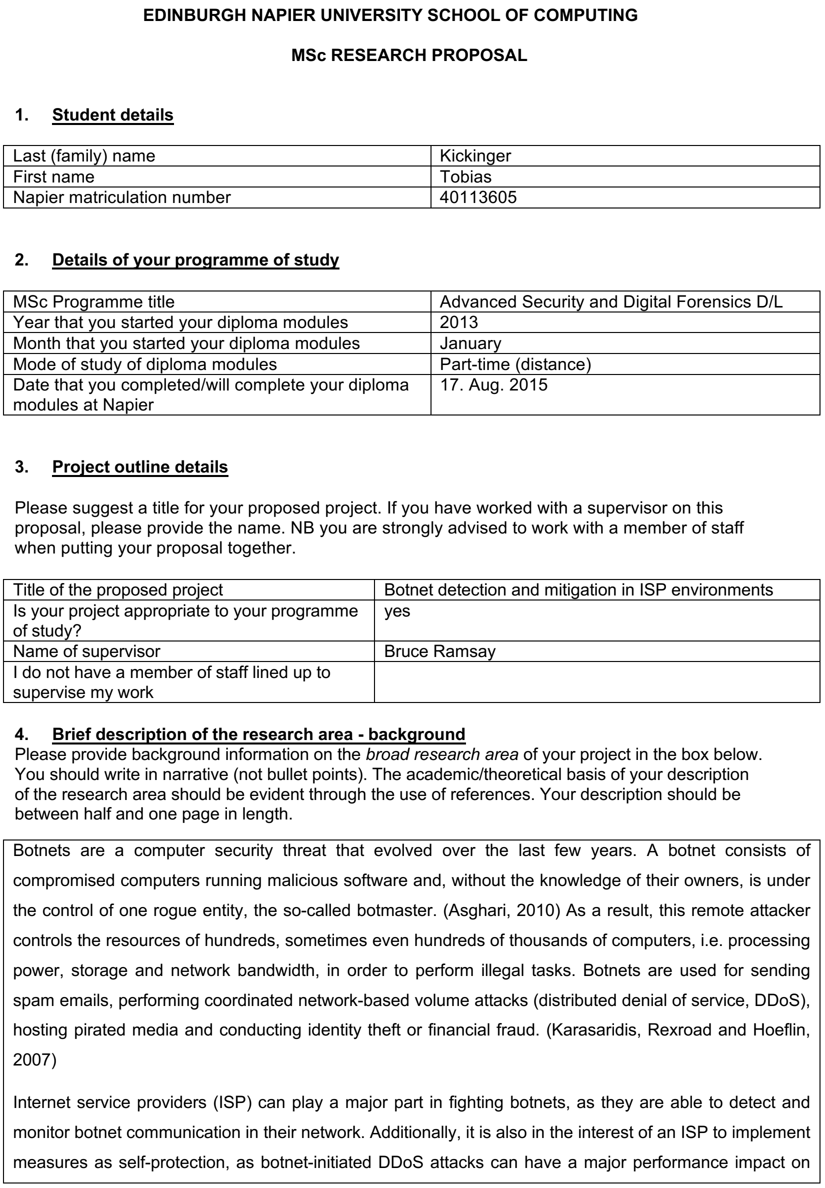
Van Eeten, M., Bauer, J. M., Asghari, H., Tabatabaie, S. and Rand, D. (2010), The role of Internet Service Providers in botnet mitigation: an empirical analysis based on spam data, TPRC.

Van Eeten, M. J. and Bauer, J. M. (2008), Economics of malware: Security decisions, incentives and externalities, Technical report, OECD Publishing.

West, M. (2008), Threats That Computer Botnets Pose to International Businesses, PhD thesis, D'Youville College.

Appendix A

Initial Project Proposal



EDINBURGH NAPIER UNIVERSITY SCHOOL OF COMPUTING

MSc RESEARCH PROPOSAL

1. **Student details**

Last (family) name	Kickinger
First name	Tobias
Napier matriculation number	40113605

2. **Details of your programme of study**

MSc Programme title	Advanced Security and Digital Forensics D/L
Year that you started your diploma modules	2013
Month that you started your diploma modules	January
Mode of study of diploma modules	Part-time (distance)
Date that you completed/will complete your diploma modules at Napier	17. Aug. 2015

3. **Project outline details**

Please suggest a title for your proposed project. If you have worked with a supervisor on this proposal, please provide the name. NB you are strongly advised to work with a member of staff when putting your proposal together.

Title of the proposed project	Botnet detection and mitigation in ISP environments
Is your project appropriate to your programme of study?	yes
Name of supervisor	Bruce Ramsay
I do not have a member of staff lined up to supervise my work	

4. **Brief description of the research area - background**

Please provide background information on the *broad research area* of your project in the box below. You should write in narrative (not bullet points). The academic/theoretical basis of your description of the research area should be evident through the use of references. Your description should be between half and one page in length.

Botnets are a computer security threat that evolved over the last few years. A botnet consists of compromised computers running malicious software and, without the knowledge of their owners, is under the control of one rogue entity, the so-called botmaster. (Asghari, 2010) As a result, this remote attacker controls the resources of hundreds, sometimes even hundreds of thousands of computers, i.e. processing power, storage and network bandwidth, in order to perform illegal tasks. Botnets are used for sending spam emails, performing coordinated network-based volume attacks (distributed denial of service, DDoS), hosting pirated media and conducting identity theft or financial fraud. (Karasaridis, Rexroad and Hoeflin, 2007)

Internet service providers (ISP) can play a major part in fighting botnets, as they are able to detect and monitor botnet communication in their network. Additionally, it is also in the interest of an ISP to implement measures as self-protection, as botnet-initiated DDoS attacks can have a major performance impact on the network infrastructure. Furthermore, high volumes of spam impair the reputation of the ISP, its customers and its IP address space, and especially the latter obstructs legitimate email transfers. (Livingood, Mody and O'Reirdan, 2012; van Eeten et al., 2010)

The effective detection and mitigation of customer-induced botnet threats poses several challenges. However, the specific requirements or restrictions that apply to ISP environments may not have been extensively covered in research so far. An ISP provides network access to its customers, so botnet detection on the endpoints itself, i.e. the computers, is hardly a feasible approach. A network-based approach is required, but due to distributed network layouts and high amounts of traffic such detection measures cannot rely on single sensors that analyse the complete traffic. Instead, solutions based on sampled network flows are required. (Moon et al., 2014)

5. Project outline for the work that you propose to complete

Please complete the project outline in the box below. You should use the emboldened text as a framework. Your project outline should be between half and one page in length.

The idea for this research arose from:

I work at an Internet Service Provider (ISP) as security engineer and hold the responsibility for security in the customer-facing wide-area networks. Attackers already use Botnet-infected customer systems to carry out various attacks and to send out spam with significant impact on the company's infrastructure and reputation. Therefore, counter-measures are required which can be implemented in an ISP environment considering its specific characteristics.

The aims of the project are as follows:

Methodological development of a measurement catalogue to minimize threats for an ISP infrastructure resulting from botnet-infected customer systems:

- A threat description of botnets and botnet-infected customer systems from an ISP perspective including a risk analysis
- A structured analysis of ISP-specific factors, requirements and restrictions for botnet detection and mitigation
- A review of possible network-based detection and mitigation approaches
- A theoretical and practical comparison of the identified approaches to detect and mitigate botnet threats
- A critical evaluation of the results considering the specific environment and recommendations for further implementation

The main research questions that this work will address include:

Which threats does an ISP face that result both from botnets in general and from botnet-infected customer systems? What are the specific requirements and restrictions for botnet detection and mitigation within an ISP environment?

Which different approaches of botnet detection are established and how can these be applied to the identified circumstances? What measures are suitable to mitigate the threat of identified botnet-infected systems?

The software development/design work/other deliverable of the project will be:
A catalogue of measurements to detect and mitigate botnet threats in an ISP environment based on a risk analysis

The project will involve the following research/field work/experimentation/evaluation:
Practical and theoretical evaluation of different detection approaches in an ISP backbone network

This work will require the use of specialist software: Network analyser

This work will require the use of specialist hardware: Carrier-grade network equipment

The project is being undertaken in collaboration with: My employer 'M-net Telekommunikations GmbH', a mid-sized ISP in Germany.

6. References

Please supply details of all the material that you have referenced in sections 4 and 5 above. You should include at least three references, and these should be to high quality sources such as refereed journal and conference papers, standards or white papers. Please ensure that you use a standardised referencing style for the presentation of your references, e.g. APA, as outlined in the yellow booklet available from the School of Computing office and http://www.soc.napier.ac.uk/~cs104/mscdiss/moodlemirror/d2/2005_hall_referencing.pdf

Asghari, H. (2010) *Botnet Mitigation and the Role of ISPs*, Delft: University of Technology.

Karasaridis, A., Rexroad, B. and Hoeflin, D. (2007) 'Wide-scale Botnet Detection and Characterization', Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets, Cambridge, p. 7.

Livingood, J., Mody, N. and O'Reirdan, M. (2012) *Recommendations for the Remediation of Bots in ISP Networks (RFC 6561)*, Internet Engineering Task Force (IETF).

Moon, Y.H., Choi, S.B., Kim, H.K. and Yoo, C. (2014) 'A Hybrid Defense Technique for ISP Against the Distributed Denial of Service Attacks', *Applied Mathematics & Information Sciences*, vol. 8, no. 5, Sep, p. 2347.

van Eeten, M., Bauer, J.M., Asghari, H., Tabatabaie, S. and Rand, D. (2010) 'The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data', WEIS.

7. Ethics

If your research involves other people, privacy or controversial research there may be ethical issues to consider (please see the information on the module website). If the answer below is YES then you need to complete a research Ethics and Governance Approval form (available on the website: http://www.ethics.napier.ac.uk).

Does this project have any ethical or governance issues related to working with, studying or observing other people? (YES/NO)	yes

8. Supervision timescale

Please indicate the mode of supervision that you are anticipating. If you expect to be away from the university during the supervision period and may need remote supervision please indicate.

Weekly meetings over 1 trimester	
Meetings every other week over 2 trimesters	x
Other	

9. Submitting your proposal

Please save this file using your surname, e.g. macdonald_proposal.doc, and e-mail it to the module leader in time for the next proposal deadline.

Appendix B

Project Management

Main Task	Deadline	CW5	CW6	CW7	CW8	CW9	CW10	CW11	CW12	CW13	CW14	CW15	CW16	CW17	CW18	CW19	CW20	CW21	CW22	CW23	CW24	CW25	CW26	CW27	CW28	CW29	CW30	CW31	CW32	CW33
		01.02.15	08.02.15	15.02.15	22.02.15	01.03.15	08.03.15	15.03.15	22.03.15	29.03.15	05.04.15	12.04.15	19.04.15	26.04.15	03.05.15	10.05.15	17.05.15	24.05.15	31.05.15	07.06.15	14.06.15	21.06.15	28.06.15	05.07.15	12.07.15	19.07.15	26.07.15	02.08.15	09.08.15	16.08.15
Initial research		■	■	■																										
Research of ISP environment				■	■	■	■	■	■	■																				
Review of relevant literature					■	■	■	■																						
Risk assessment								■	■	■	■	■																		
Thesis: Literature Review	03.05.15											■	■	■	■															
Initial Report	10.05.15															■														
Thesis: Methodology	31.05.15																■	■	■											
Thesis: Analysis and results	05.07.15																			■	■	■	■	■						
Thesis: Discussion	19.07.15																								■	■				
Thesis: Introduction	02.08.15																										■	■		
Thesis: Conclusion	02.08.15																										■	■		
Thesis: Abstract	09.08.15																												■	
Buffer																														■