UNIVERSITY OF SOUTHAMPTON

FACULTY OF PHYSICAL AND APPLIED SCIENCES

Electronics and Computer Science

Distributed Denial-of-Service Attack Trends, Detection and Mitigations Strategies

by

Fatih Uyaroglu

A dissertation submitted for the award of
MSc Cyber Security

Supervisor: Prof. Dr. Vladimiro Sassone
Examiner: Prof. Dr. Ed Zaluska

September 2, 2016

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF PHYSICAL AND APPLIED SCIENCES
Electronics and Computer Science

A dissertation submitted for the award of MSc Cyber Security

DISTRIBUTED DENIAL-OF-SERVICE ATTACK TRENDS, DETECTION AND MITIGATIONS STRATEGIES

by Fatih Uyaroglu

Over the past few years, the size of distributed denial of service (DDoS) attacks has increased dramatically. Recently, DDoS attackers have the ability to generate malicious network traffic that reaches up to 500 Gbps. Moreover, internet protocols, websites and the OSI (Open Systems Interconnection) layers have several security weaknesses. DDoS attackers try to find advanced techniques in order to exploit these weaknesses and initiate devastating DDoS attacks. Several DDoS protection mechanisms have been proposed to deal with massive DDoS attacks; however, it is extremely hard to develop a comprehensive defence mechanism due to the diversity of attack techniques. Therefore, this research targets to examine latest DDoS trends and evaluate existing detection/mitigation solutions. In this dissertation, firstly, some of the most destructive DDoS attack types are comprehensively explained. Then, botnets and how attackers use them to launch massive DDoS attacks are explained in detail. Afterwards, latest DDoS attacks are analysed to understand DDoS trends and exploited vulnerabilities. Finally, some of the most efficient DDoS detection/mitigation techniques are analysed to reveal their limitations and strengths.

Contents

List of Figures

Acknowledgements

I would first like to offer my deepest thanks to my dissertation supervisor, Prof. Dr. Vladimiro Sassone, for his polite behaviour, assistance and positive guidance during my research process. I would also like to offer my deepest thanks to my second supervisor, Prof. Dr. Ed Zaluska, for giving positive feedback and support during my dissertation and writing process.

I would especially give my special thanks to my family members and aunt for their encouragement and assistance throughout my life.

I would also give my special thanks to my sponsor and managers for giving encouragement and providing financial support.

Finally, I would like to send my sincerest thanks to Dr. Md. Sadek Ferdous and Dr. Mustafa Cagri Kutlu for their assistance and positive feedback throughout my research.

Chapter 1

Introduction

1.1 Introduction to Distributed Denial-of-Service (DDoS) Attacks

The rapid growth of innovative services that are provided over computer networks facilitates the life of the people who use these services. However, innovative developments have engendered extra attack opportunities for cyber criminals due to the weaknesses of these developments (Jun et al., 2014). Distributed denial-of-service (DDoS) attacks are launched to exhaust the system resources of targets such as memory, network bandwidth and CPU (Srivastava et al., 2011). Attackers can quickly stop the services of targeted computer networks by generating vast volumes of network traffic and sending this generated traffic to their targets. Therefore, attackers can cause lethal damage to the critical infrastructures of companies and governments by preventing the crucial operations of victim servers. Moreover, DDoS attacks have the capability to cause both massive economic and prestige losses to the victims of these type of attacks (Jun et al., 2014). The OSI (Open Systems Interconnection) layers and commonly used internet protocols have several vulnerabilities that can be exploited by attackers in order to initiate massive DDoS attacks. It is extremely difficult to defend against DDoS attacks and develop an extensive DDoS protection strategy because each type of DDoS attack has different structures and detection/mitigation mechanisms. In addition, eliminating the threats emerged because of DDoS attacks requires a comprehensive research. Therefore, in order to develop an extensive protection and mitigation strategy, types of DDoS attacks and latest DDoS trends should be analysed comprehensively. Moreover, botnets and their communication mechanisms should also

be examined carefully. Additionally, current DDoS attack mitigation mechanisms should be analysed to reveal their limitations and strengths. Then, the results of the analysis can be used in order to discover existing problems and develop more effective mitigation mechanisms.

1.2 Distributed Denial-of-Service (DDoS) Background

Distributed denial-of-service (DDoS) attacks initially appeared as a type of cyber attacks that generate massive volumes of network traffic towards predetermined targets (Jun et al., 2014). In February 2000, the websites of Amazon and Yahoo were crashed by DDoS attacks. These are the first widely known DDoS attacks and various DDoS tools such as Stacheldracht, Trinoo, Tribe Flood Network (TFN), Trinity and TFN 2000 (TFN2K) were utilized in conducting these attacks (Jun et al., 2014). At that time, researchers and security analysts were trying to develop anomaly based detection mechanisms in order to detect DDoS attacks. It was achievable to discover DDoS attacks with anomaly based detection mechanisms; however, it was extremely challenging to efficiently mitigate or block these types of attacks. The reason was that even if it was achievable to detect DDoS attacks, analysis techniques were insufficient to correctly determine the malicious IP packets because of IP spoofing techniques (Jun et al., 2014). Internet worms exploit the vulnerabilities of computer systems and take vulnerable systems over quickly. For instance, a network worm called Slammer infected approximately 75.000 internet servers in less than 10 minutes, causing the infected servers to crash (Jun et al., 2014). Advanced types of DDoS attacks have appeared since 2000. Nowadays, the attackers generally do not prefer to generate vast volumes of network traffic in order to crash the whole victim network, but they try to make a certain application layer service unavailable to its legitimate users. In application layer attacks, if the DDoS attackers generate malicious network traffic in an advanced way, they could quickly crash application layer services using relatively low attack traffic bandwidth. It is quite difficult to distinguish malicious attack packets from normal packets in application layer attacks because malicious attack packets complete each procedure that is required to be legitimate. Therefore, it is extremely challenging to discover an application layer attack utilizing only broadly used DDoS defence mechanisms such as packet based detection techniques and analysing the bandwidth of attack traffic (Jun et al., 2014).

In July 2009, a series of massive DDoS attacks were initiated against financial, media and government websites in the U.S.A and South Korea utilizing huge botnets. In this example, the attackers carried out several types of DDoS attacks such as UDP flooding, ICMP flooding, TCP SYN flooding and HTTP GET flooding (Jun et al., 2014). Among these types, the ones that target HTTP protocol were not efficiently avertible because traditional DDoS protection methods are insufficient to discover and stop devastating application layer attacks. The reason of this is that nearly all DDoS defence mechanisms are based on network traffic volume and bandwidth abnormality. Although the total amount of malicious traffic was immense, traditional DDoS defence mechanisms failed to discover the attackers because each attack system did not generate such heavy traffic that could be detected. Therefore, application behaviour based detection mechanisms should be developed in order to detect and mitigate application layer attacks (Jun et al., 2014).

1.3 Dissertation Aims and The Scope of Research

The objective of this dissertation is to present comprehensive information about distributed denial of service (DDoS) attacks and the crucial role of botnets in conducting these type of attacks. Furthermore, this dissertation also presents extensive information about the latest DDoS attack trends and the weaknesses exploited in latest attacks. Additionally, it targets to explain some of the most important DDoS defence and mitigation mechanisms in order to reveal their strengths and limitations.

The main scope of this research is defined below:

- Explaining the definition and significance of distributed denial of service (DDoS) attacks.
- Explaining the main steps of DDoS attacks which are followed by DDoS attackers.
- Understanding the structure of botnet based DDoS attacks.
- Classifying botnet based DDoS attacks according to the communication mechanisms utilized in conducting these type of attacks.

- Defining the classification of botnet based DDoS attacks based on the exploited vulnerability.
- Explaining the architectural designs of botnet control and command (C&C) mechanisms.
- Discovering the latest botnet based DDoS attack trends in Q1 2016.
- Defining the classification of DDoS attack types by OSI (Open Systems Interconnection) layers.
- Explaining the classification & comparison of botnet based DDoS attacks detection methods (Signature-based detection and Anomaly-based Detection).
- Explaining some of the most important DDoS protection and mitigation mechanisms and making comparisons between these mechanisms.

1.4 The Outline of Dissertation

In the second chapter, the definition and importance of DDoS attacks are explained in detail. Additionally, the main steps which need to be completed by attackers in order to launch a DDoS attack are also explained in this chapter. Then, in the third chapter, DDoS attacks are classified according to the communication mechanisms used in carrying out these types of attacks. Moreover, DDoS attacks are also classified based on the exploited weaknesses and OSI (Open Systems Interconnection) layers. After that, in the fourth chapter, the term botnet, botnet structure and how botnets are utilized in massive DDoS attacks are explained in detail. Furthermore, latest trends in carrying out botnet based DDoS attacks are analysed according to the Kaspersky Lab's DDoS Intelligence Report that is based on the trends in the first quarter of 2016. In the fifth chapter, botnet based DDoS attacks detection methods (Anomaly-based Detection and Signature-based Detection) are defined and comparisons are also made between this two detection method in order to reveal their strengths and weaknesses. Additionally, some of the most important DDoS mitigation and protection mechanisms are defined and compared in order to show their limitations and strengths. Finally, conclusions and recommendations are given in chapter six based on the research conducted throughout this dissertation process.

Chapter 2

Distributed Denial-of-Service (DDoS) Attacks

This chapter firstly introduces the significance and definition of DDoS attacks. Afterwards, the elements that compose a DDoS attack are demonstrated. Finally, the steps of DDoS attacks are explained in detail.

2.1 The Significance of Distributed Denial of Service (DDoS) Attacks

The number of Distributed Denial of Service (DDoS) attacks and their impacts on victim systems has been increasing extraordinarily over the last few years. The rapid development of internet protocols, computer systems and networks have engendered new DDoS opportunities for attackers because of the security vulnerabilities of new developments. Attackers try to discover the security vulnerabilities of computer systems and internet protocols in order to launch Distributed Denial of Service attacks against governments, banks and profitable enterprises (Behal and Kumar, 2016). DDoS attacks have caused huge financial damages to the victims of these attacks during the past few years. According to the study which was carried out by Kaspersky (2014), a DDoS attack results in approximately $444.000 in financial loss and IT expenditure for large enterprises. Moreover, according to the survey of Kaspersky (2015), 50% of the enterprises examined have faced some problems and service interruptions because of a Distributed Denial of

Service (DDoS) attack conducted in the previous year. A study carried out by Arbor Networks (2016) illustrate the remarkable increase in the size of latest DDoS attacks as shown in Figure 2.1 below.

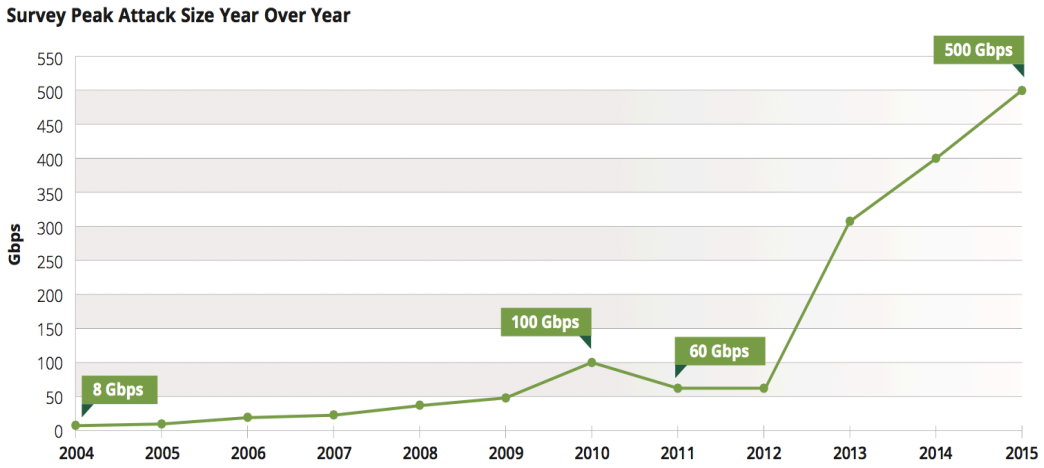

Figure 2.1: Increase in the size of latest DDoS attacks (Arbor Networks, 2016).

2.2 The Definition of Distributed Denial of Service (DDoS) Attack

Denial of Service (DoS) attack is a technique for preventing access to a service or website content by stopping their operation (CERT-UK, 2014). When an attacker launches a DoS attack from more than one device such as a computer or smart phone at the same time, this initiated DoS attack turns into a Distributed Denial of Service (DDoS) attack (CERT-UK, 2014). Attackers initiate DDoS attacks to generate massive amounts of unrequested network traffic and exhaust the resources of victim systems such as CPU, network bandwidth, system memory and cache (Srivastava et al., 2011). The intention of an attacker who launches a DDoS attack is to deny legitimate users' access to the services provided by the victim server (Srivastava et al., 2011). DDoS attackers have the ability to use large numbers of compromised devices located all over the world and initiate devastating DDoS attacks against various victims simultaneously. The Internet's infrastructure was not designed securely, and attackers try to discover the weaknesses of this insecure infrastructure in order to exploit these weaknesses (Douligeris and Mitrokotsa, 2004). Computer networks have limited sources, and vast amounts of network traffic could exhaust the sources of any victim network (Douligeris and

Mitrokotsa, 2004). Attackers use spoofed IP addresses, anonymity and botnets in DDoS attacks; therefore, it is extremely hard to distinguish legitimate network traffic from malicious network traffic (Douligeris and Mitrokotsa, 2004).

Four elements which compose a Distributed Denial of Service (DDoS) attack are represented in Figure 2.2 below. These are the attacker, the handlers/masters, the agents/zombies and a victim/target. The handlers/masters are compromised devices, and a malicious code runs on them in order to control attack agents (Douligeris and Mitrokotsa, 2004). The agents/zombies are also compromised devices, and they are managed by handlers/masters in order to generate traffic towards the predetermined target.

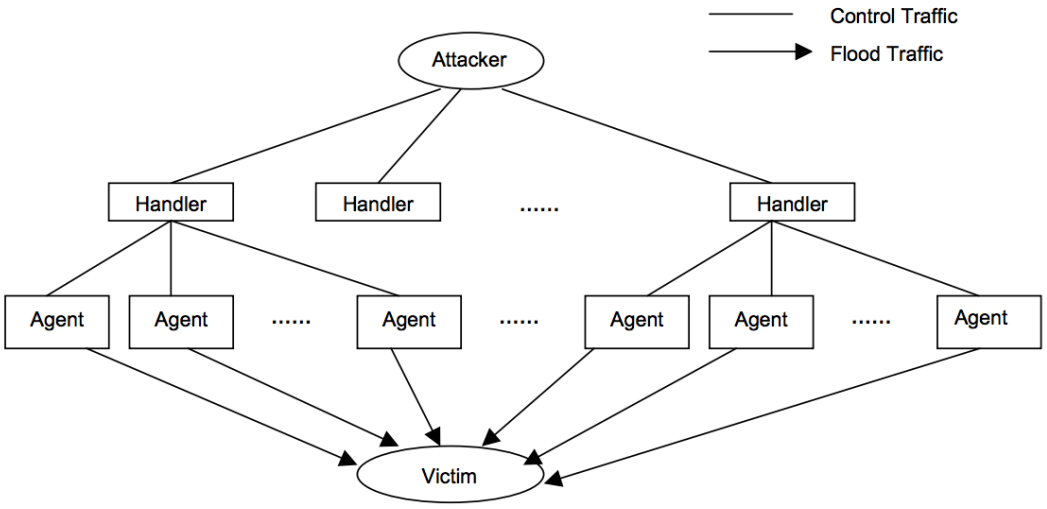

Figure 2.2: The Architecture of Distributed Denial of Service attacks. (Douligeris and Mitrokotsa, 2004)

2.3 The Steps of a Distributed Denial of Service (DDoS) Attack Mechanism

There are four main steps which are followed by attackers in order to prepare and carry out a Distributed Denial of Service (DDoS) attack. These main steps are:

1. Collection of Agents: The agents which will be used to conduct a DDoS attack are determined by an attacker in this step. The aim of attackers is to take control of vulnerable computer systems; therefore, they try to detect weaknesses of these systems in order to make them agents (Douligeris and

Mitrokotsa, 2004). Vulnerability scanning tools are also used by attackers to automate this process. Agents should have the ability to produce destructive network traffic; hence, the resources of controlled agents should be sufficient to perform a DDoS attack (Douligeris and Mitrokotsa, 2004).

2. Compromise: When attackers detect the security weaknesses of computer systems, they try to exploit these weaknesses and execute a malicious program in order to establish the attack code which will be used for launching DDoS attacks (Douligeris and Mitrokotsa, 2004). Moreover, attackers try to prevent their attack code from being detected and deactivated. Attackers also use malicious codes such as Code Red and Ramen worm to automate this compromise step. The owners of the compromised agent hosts generally do not know that their hosts have been compromised, and their systems will be used to conduct DDoS attacks. When taking part in a Distributed Denial of Service (DDoS) attack, agent systems do not consume large amounts of system resources, and the users of these agent systems do not experience performance problems (Douligeris and Mitrokotsa, 2004).

3. Communication: DDoS Attackers communicate with a large number of masters/handlers to determine which agents are online and ready to launch an attack (Douligeris and Mitrokotsa, 2004). Furthermore, attackers also determine when to update agents and when to initiate a DDoS attack by communicating with handlers. Agents can communicate with one or more handler(s) depending on the configuration of the attack network. UDP, ICMP and TCP protocols are commonly used in the communication method established between the handlers/masters and the agents and between the attacker and the masters/handlers (Douligeris and Mitrokotsa, 2004).

4. Attack: The attacker defines the victim and the features of the DDoS attack such as duration, type, size, TTL and port numbers at this step. DDoS attacks have a lot of features, and the features of a DDoS attack can be easily modified by attackers to avoid being detected (Douligeris and Mitrokotsa, 2004). Attackers also use communication protocols such as Internet Relay Chat (IRC) to communicate with the handlers and the agents, and IRC protocol provides vital advantages when conducting a DDoS attack. For example, IRC provides a high level of anonymity to the DDoS attacker; therefore, DDoS attacks could not be easily analysed and the attacker could not be easily detected (Douligeris and Mitrokotsa, 2004). Moreover, IRC protocol offers a powerful and guaranteed mechanism for message distribution.

Chapter 3

Classification of Distributed Denial-of-Service (DDoS) Attacks

This chapter presents detailed information about the classification of DDoS attacks. It firstly classifies DDoS attacks based on their communication methods. Then, DDoS attack types are also classified according to the exploited vulnerabilities. Finally, these attacks are classified according to the OSI (Open Systems Interconnection) layers.

3.1 Classification of DDoS Attacks According to Communication Methods

Distributed Denial of Service (DDoS) attacks are basically separated into two types according to the communication method established between the handlers/masters and the agents/zombies (Hashmi et al., 2012). These types are indirect communication based DDoS attacks and direct communication based DDoS attacks.

In a direct communication based DDoS attack, the handlers/masters and agents/-zombies need to be aware of one another's identity to communicate during DDoS attacks. This is accomplished by embedding the details of the handler devices such as IP address in the malicious attack program that will be installed on agent devices (Hashmi et al., 2012). The structure of a direct communication based DDoS attack is shown below in Figure 3.1.

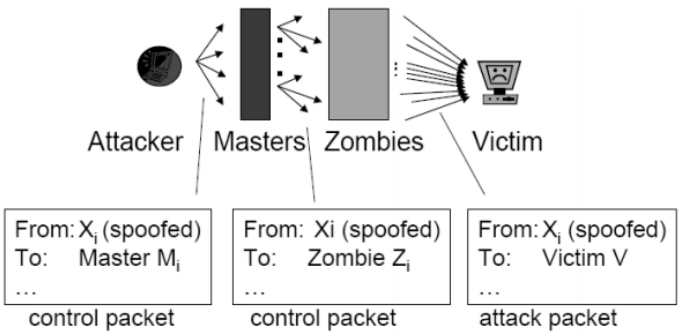

Figure 3.1: The structure of a direct communication based DDoS attack (Hashmi et al., 2012).

The shortcoming of the direct communication based DDoS attack is that detection of a compromised device may lead to the disclosure of the whole DDoS attack structure (Hashmi et al., 2012). Furthermore, the handlers/masters and agents/zombies listen for incoming network connections to communicate with each other; therefore, network monitoring tools can discover the agents/zombies and the masters/handlers which are used in a direct communication based DDoS attack (Hashmi et al., 2012).

In indirect communication based DDoS attacks, reflectors are used for indirection to boost the life span of the DDoS attack network. Moreover, attackers also benefit from communication protocols such as Internet Relay Chat (IRC) to provide a powerful handler/agent communication (Hashmi et al., 2012). IRC channels also offer a high level of anonymity to DDoS attackers; therefore, the structure of DDoS attacks could not be examined and revealed easily. Furthermore, the attack traffic of the DDoS network could not be differentiated from legitimate users' network traffic easily because DDoS agents make connections to a common port which is controlled by a legitimate service (Hashmi et al., 2012). In this type of DDoS attacks, attackers can generate requests by embedding the victim's IP address into network packets and send these generated request packets to the reflectors such as NTP and DNS servers. When the reflectors get requests, they send overwhelming responses to the victim's IP address. The structure of an indirect communication based DDoS attack is shown below in Figure 3.2.

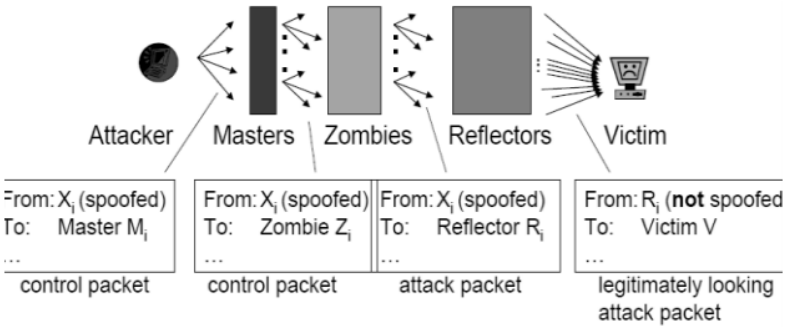

Figure 3.2: The structure of an indirect communication based DDoS attack (Hashmi et al., 2012).

3.2 Classification of DDoS Attacks Based on the Exploited Vulnerability

It is extremely challenging to deal with and analyse DDoS attacks due to the distributed structure of DDoS attacks (Zargar et al., 2013). Moreover, DDoS attackers commonly use spoofed IP addresses to conceal their real identities; hence, the examination of DDoS attacks becomes more challenging (Zargar et al., 2013). Computers connected to the Internet have security vulnerabilities that attackers can exploit, and the occurrence of DDoS attacks conducted at the application layer are growing very quickly. Therefore, understanding the security vulnerabilities of computer systems and how these vulnerabilities are exploited to carry out DDoS attacks are crucial steps for developing more efficient DDoS defence strategies (Zargar et al., 2013).

DDoS attacks can be separated into four attack groups according to the exploited security vulnerability. These attacks are: protocol exploit attacks, flood attacks, malformed packet attacks and amplification attacks (Douligeris and Mitrokotsa, 2004).

3.2.1 Flood Attack

In these type of attacks, the agents generate huge volumes of network packets and send these packets to a target in order to consume the target's network bandwidth (Douligeris and Mitrokotsa, 2004). Huge volumes of network packets may crash or slow down the target system; therefore, the target system could not respond to legitimate users' requests. ICMP flood attacks and UDP flood attacks are examples of most known flood attacks (Douligeris and Mitrokotsa, 2004).

- User Datagram Protocol (UDP) Flood Attack: UDP flood occurs when vast amounts of UDP network packets being sent to a target system. Attackers overwhelm specific or random ports of the target system with network packets which contain UDP data (Imperva, 2016). This attack leads to the consumption of available network bandwidth which is required for legitimate users' requests. In UDP flood attacks, UDP packets can be directed to either specific or random ports of the target system; however, random target ports are typically used when conducting these types of attacks (Douligeris and Mitrokotsa, 2004). When the target system gets UDP packets, the application which is running on the targeted port is determined by the target system. If there is not any application which is running on the targeted port, the victim generates an ICMP destination unreachable message and send it to the fake source address (Douligeris and Mitrokotsa, 2004). If massive amounts of UDP packets being sent to the ports of the target, this target system will eventually crash. IP spoofing technique can be used by attackers in order to modify the source IP of the DDoS attack packets with the help of DDoS attack tools. By this way, the real identity of the agents is prevented from being disclosed and the response packets of the target systems are not directed to the attack agents (Douligeris and Mitrokotsa, 2004). UDP Protocol does not need a three-way handshake mechanism like TCP protocol; therefore, UDP Protocol is optimal for network traffic which does not need to be verified and controlled such as VoIP (Imperva, 2016). However, UDP Protocol becomes more vulnerable to exploitation due to the absence of three-way handshake mechanism. Therefore, vast volumes of network packets can be sent without any limitation to a victim system over UDP channels (Imperva, 2016). An example of UDP flood attack structure is illustrated below in Figure 3.3.

- Internet Control Message Protocol (ICMP) Flood Attack: ICMP flood attacks exploit the vulnerabilities of ICMP protocol that enables to send echo packets to remote computers. In ICMP flood attacks, attackers commonly send huge volumes of fake ICMP_ECHO_REPLY packets to the broadcast IP addresses of victim computer networks (Douligeris and Mitrokotsa, 2004). These fake packets wait response from the victim network and all of the computers on the victim network send a reply to these fake packets. This situation leads to the consumption of the victim's outgoing and incoming network bandwidth (Srivastava et al., 2011). An example of ICMP flood attack structure is illustrated below in Figure 3.4.

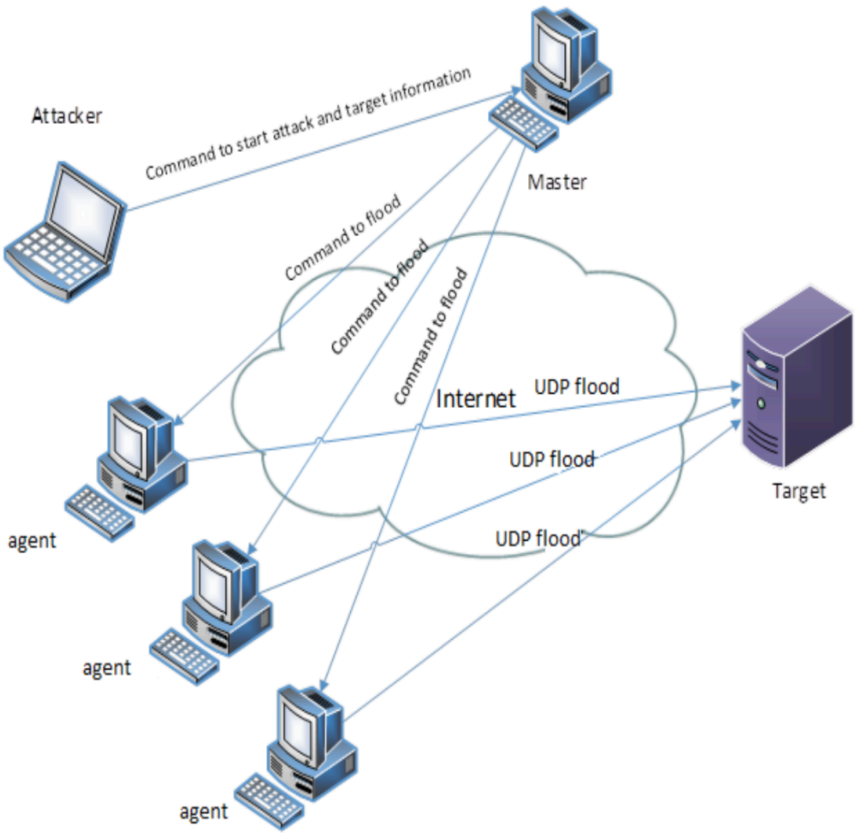

Figure 3.3: An example of UDP flood attack structure. (Telelink, 2013)

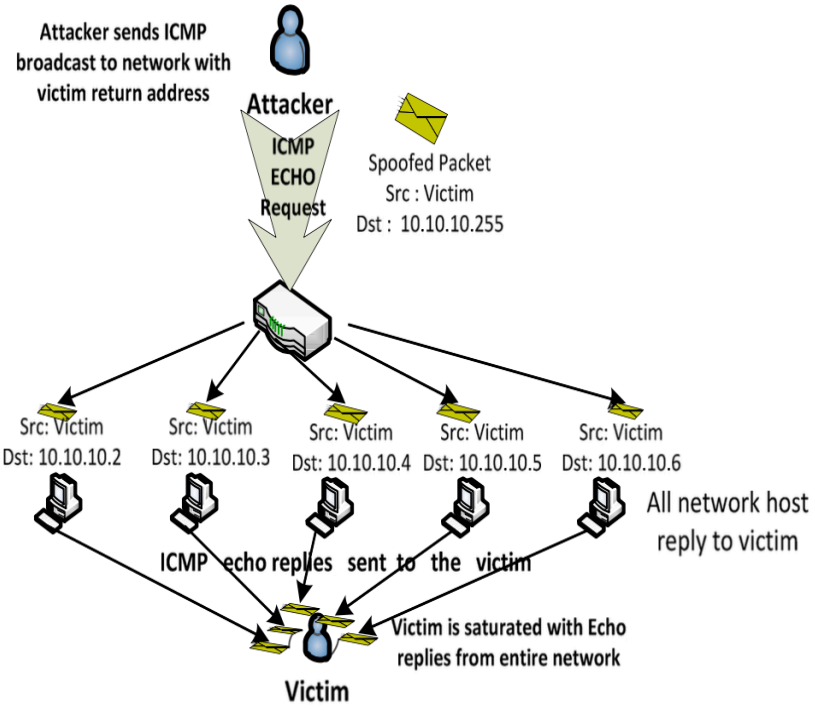

Figure 3.4: An example of ICMP flood attack structure. (Wong and Tan, 2014)

3.2.2 Amplification Attack

UDP based network protocols do not need a three-way handshake mechanism to confirm the sender's identification information such as IP address. DDoS attackers typically exploit the weaknesses of UDP based network protocols in order to conduct amplified DDoS attacks that generate up to 500 Gbps of malicious network traffic (Kührer et al., 2014). In amplified DDoS attacks, attackers generate network packets with spoofed source IP addresses and send them to many reflectors, such as DNS servers and web servers, that reflect the network traffic to the target systems. Reflectors that generate extremely large responses to the ordinary requests are called as amplifiers and chosen by attackers to initiate amplified DDoS attacks (Kührer et al., 2014). Public NTP servers and open recursive DNS resolvers are commonly used in DDoS attacks as an amplifier due to their amplification characteristic. By using IP spoofing, attackers enforce amplifiers to amplify and reflect malicious network traffic to the target systems (Kührer et al., 2014). DNS amplification attack structure is illustrated below in Figure 3.5.

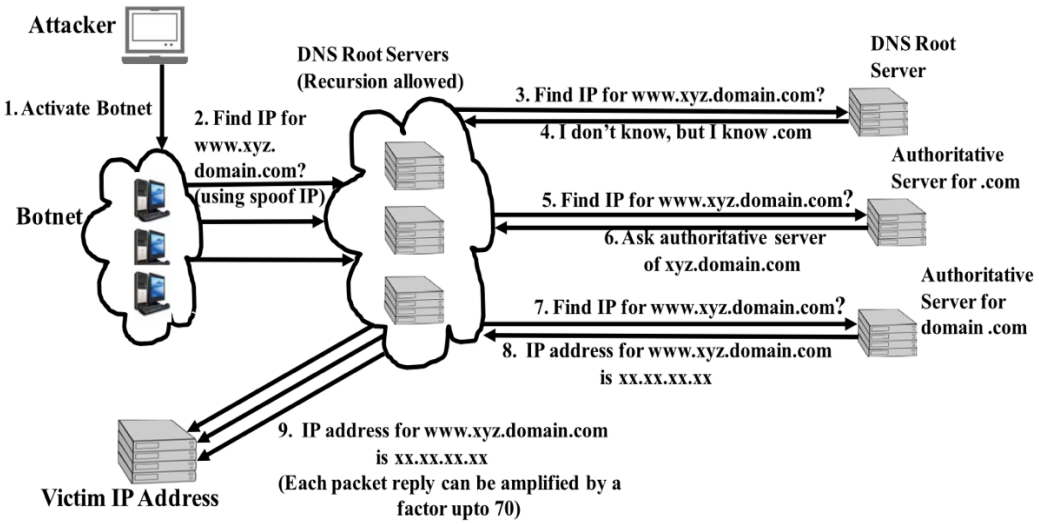

Figure 3.5: DNS amplification attack structure. (Hoque et al., 2015)

DDoS amplification attacks have the ability to create huge volumes of network traffic; therefore, these types of attacks can consume the network bandwidth of target system very quickly. Attackers use IP spoofing and amplifiers in DDoS amplification attacks; therefore, the examination of amplification attacks and the disclosure of the whole DDoS amplification attack structure are extremely difficult (Kührer et al., 2014). Moreover, botnets are extensively used in DDoS amplification attacks to increase the attack size and lengthen the life span of the amplification

attack (Zargar et al., 2013). According to the report of Arbor Networks (2016), most commonly used protocols for amplification/reflection are illustrated below in Figure 3.6. Additionally, the table of well known protocols and their bandwidth amplification factors are illustrated below in Figure 3.7. For example, NTP protocol's bandwidth amplification factor is 556.9; therefore, this protocol has the ability to amplify each response packet by an amplification factor up to 556.9.

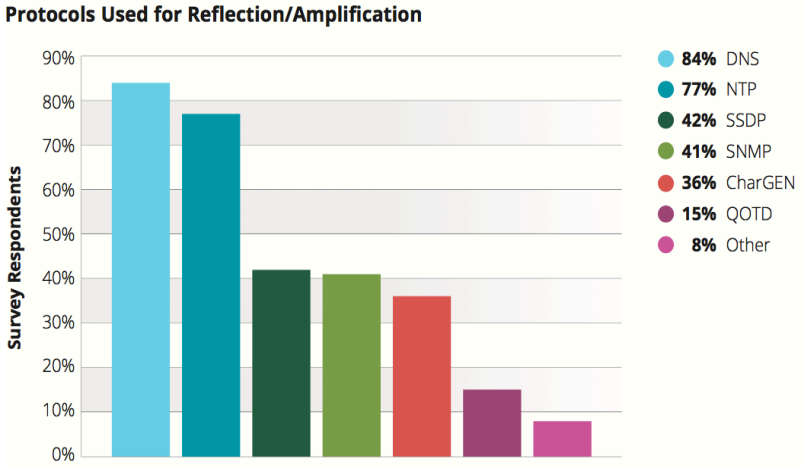

Figure 3.6: Most commonly used protocols for amplification. (Arbor Networks, 2016)

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request

Figure 3.7: Well-known protocols and their bandwidth amplification factors. (US-CERT, 2015)

3.2.3 Protocol Exploit Attack

These types of attacks exploit particular characteristics and architectural security bugs of vulnerable protocols established at the target system in order to exhaust huge amounts of vital system resources (Douligeris and Mitrokotsa, 2004). TCP SYN attacks, PUSH + ACK attacks, the authentication server attacks and CGI request attacks are the most well-known examples of protocol exploit attacks.

- TCP/SYN Attack: These types of attacks exploit the built-in vulnerability of the three-way handshake mechanism used in the establishment of a Transmission Control Protocol (TCP) connection (Douligeris and Mitrokotsa, 2004). A classic three-way handshake mechanism between the server and a legitimate system user starts with the connection request of the legitimate system user (Darwish et al., 2013). This connection request is made by sending a synchronization (SYN) packet to the server. After accepting the initial SYN packet of the legitimate user, the server sends back a synchronize/acknowledge (SYN/ACK) packet to the legitimate user. In the last step of three-way handshake mechanism, the legitimate system user sends the final acknowledge (ACK) packet to the server in order to establish the TCP connection (Darwish et al., 2013). An attacker launches a SYN flood attack by generating vast volumes of SYN packets and sending them to the target system but never replies back with the ACK packets. Therefore, the three-way handshake process could not be completed, and the target system starts waiting for the acknowledge (ACK) packets (Darwish et al., 2013). As a result of this, the target server's buffer which is used for new incoming connections gets overloaded, and the target could not process legitimate users' requests because of the overloaded buffer (Douligeris and Mitrokotsa, 2004). Furthermore, SYN flood attacks can also be conducted by generating network packets with spoofed IP address. The three-way handshake mechanism and SYN flood attack are illustrated respectively below in Figure 3.8(a) and Figure 3.8(b).

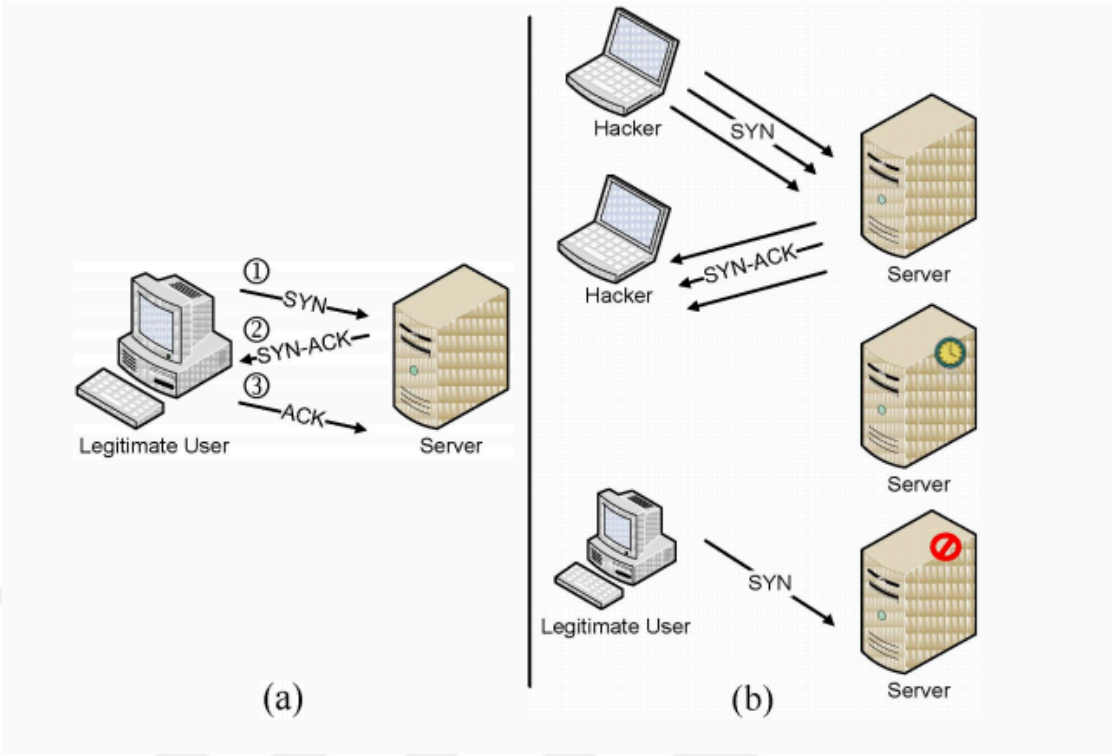

Figure 3.8: The three-way handshake mechanism and SYN flooding attack. (Darwish et al., 2013)

3.2.4 Malformed packet attacks

In malformed packet attacks, IP packets are generated with incorrect information and these spoofed packets are sent to the target using agents in order to slow down and crash the target system (Douligeris and Mitrokotsa, 2004). These attacks can be separated into two groups of attacks: IP packet options attack and IP address attack (Douligeris and Mitrokotsa, 2004). In IP address attacks, packets are generated with the same destination and source IP address. As a result of this, the operating system of targets becomes confused and target systems get crashed (Douligeris and Mitrokotsa, 2004). In IP packet options attacks, the optional fields of a packet can be randomized and each quality of service bit can be set to one. This increase the processing time which is used for analysing the network traffic (Douligeris and Mitrokotsa, 2004). Therefore, if these attacks are conducted with large numbers of agents, the target system can be crashed.

3.3 DDoS Attack Types by OSI (Open Systems Interconnection) Layers

Botnet based DDoS attacks can also be separated into three main categories according to OSI (Open Systems Interconnection) layers. These main categories are: Application Layer DDoS attacks, Network Layer DDoS attacks and Transport Layer DDoS attacks. In application layer attacks, cyber criminals use application layer (Layer 7) protocols such as HTTPS, HTTP, DNS, FTP and SMTP in order to generate network traffic towards the predetermined target (Bhattacharyya and Kalita, 2016). This malicious traffic typically includes CPU intensive requests and these requests are sent to the predetermined target in order to make it unavailable. In application layer attacks, the total traffic volume required to slow down and crash a target is relatively lower than the total traffic volume that is needed in other types of OSI layer attacks such as network layer attacks (Bhattacharyya and Kalita, 2016). Therefore, application layer DDoS attacks are the most devastating types of DDoS attacks and becoming more sophisticated. Moreover, application layer attack traffic could not be distinguished from legitimate users' traffic; hence, it is extremely difficult to analyse and detect this type of malicious traffic. In transport and network layer attacks, attackers try to consume resources such as the memory of security devices like switches, firewalls and routers and the network bandwidth of the target. To perform a destructive attack, the agents send vast volumes of traffic through the transport layer and network layer to the target (Bhattacharyya and Kalita, 2016). The size of these types of attacks can reach up to 500 Gbps (Arbor Networks, 2016). TCP (Transmission Control Protocol), UDP (User Datagram Protocol) and ICMP (Internet Control Message Protocol) are commonly used in these type of attacks. UDP flood, TCP SYN flood, NTP, ICMP echo and DNS amplification are the most popular attacks conducted over the network layer (Bhattacharyya and Kalita, 2016). The layers of the OSI (Open Systems Interconnection) model and attack possibilities by these layers are illustrated respectively below in Figure 3.9 and Figure 3.10.

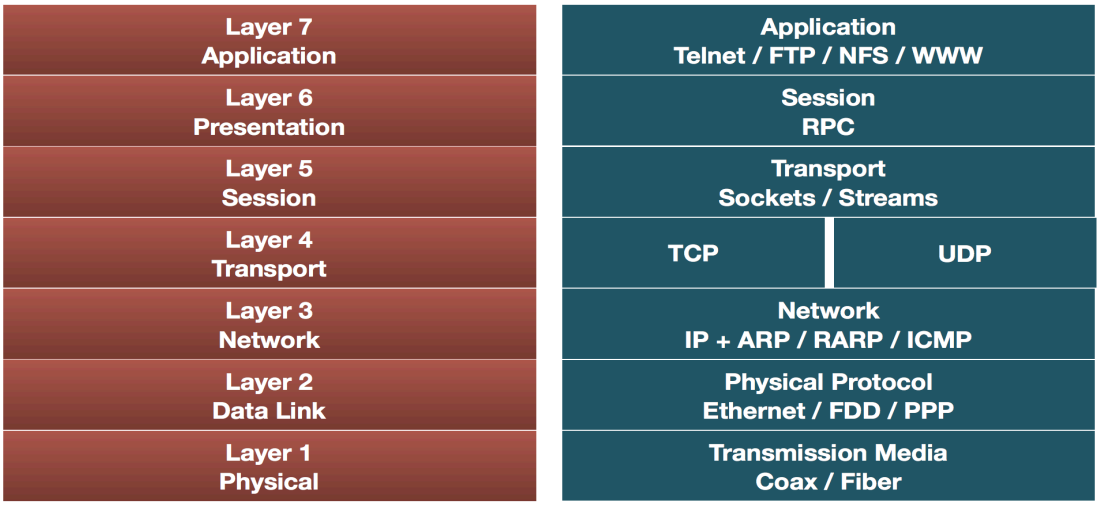

Figure 3.9: The layers of the OSI (Open Systems Interconnection) model. (Alam, 2014)

Attack Possibilities by OSI Layer

OSI Layer	Protocol Data Unit (PDU)	Layer Description	Protocols	Examples of Denial of Service Techniques at Each Level	Potential Impact of DoS Attack	Mitigation Options for Attack Type
Application Layer (7)	Data	Message and packet creation begins. DB access is on this level. End-user protocols such as FTP, SMTP, Telnet, and RAS work at this layer	Uses the Protocols FTP, HTTP, POP3, & SMTP and its device is the Gateway	PDF GET requests, HTTP GET, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)	Reach resource limits of services Resource starvation	Application monitoring is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDoS attacks
Presentation Layer (6)	Data	Translates the data format from sender to receiver	Uses the Protocols Compression & Encryption	Malformed SSL Requests -- Inspecting SSL encryption packets is resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server	The affected systems could stop accepting SSL connections or automatically restart	To mitigate, consider options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in protected memory on a secure bastion host
Session (5)	Data	Governs establishment, termination, and sync of session within the OS over the network (ex: when you log off and on)	Uses the Protocol Logon/Logoff	Telnet DDoS-attacker exploits a flaw in a Telnet server software running on the switch, rendering Telnet services unavailable	Prevents administrator from performing switch management functions	Check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability
Transport (4)	Segment	Ensures error-free transmission between hosts: manages transmission of messages from layers 1 through 3	Uses the Protocols TCP & UDP	SYN Flood, Smurf Attack	Reach bandwidth or connection limits of hosts or networking equipment	DDoS attack blocking, commonly referred to as blackholing, is a method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. Black holding is typically deployed by the ISP to protect other customers on its network from the adverse effects of DDoS attacks such as slow network performance and disrupted service
Network (3)	Packet	Dedicated to routing and switching information to different networks. LANs or internetworks	Uses the Protocols IP, ICMP, ARP, & RIP and uses Routers as its device	ICMP Flooding - A Layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth	Can affect available network bandwidth and impose extra load on the firewall	Rate-limit ICMP traffic and prevent the attack from impacting bandwidth and firewall performance
Data Link (2)	Frame	Establishes, maintains, and decides how the transfer is accomplished over the physical layer	Uses the Protocols 802.3 & 802.5 and it's devices are NICs, switches bridges & WAPs	MAC flooding -- inundates the network switch with data packets	Disrupts the usual sender to recipient flow of data -- blasting across all ports	Many advances switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations; allow discovered MAC addresses to be authenticated against an authentication, authorization and accounting (AAA) server and subsequently filtered
Physical (1)	Bits	Includes, but not limited to cables, jacks, and hubs	Uses the Protocols 100Base-T & 1000 Base-X and uses Hubs, patch panels, & RJ45 Jacks as devices	Physical destruction, obstruction, manipulation, or malfunction of physical assets	Physical assets will become unresponsive and may need to be repaired to increase availability	Practice defense in-depth tactics, use access controls, accountability, and auditing to track and control physical assets

Figure 3.10: Attack possibilities by Open System Interconnection (OSI) layers. (US-CERT, 2014)

Most of the earlier DDoS attacks were typically conducted over the network and transport layer (OWASP, 2010; Alam, 2014). However, current DDoS mitigation strategies are beneficial in combating transport layer and network layer attacks; therefore, attackers have started to focus on application layer attacks (Suryawanshi and Todmal, 2015; OWASP, 2010). According to the report of Arbor Networks (2016), most commonly exploited protocols for launching application layer attacks are illustrated below in Figure 3.11. Additionally, an example of application layer attack architecture is illustrated below in Figure 3.12.

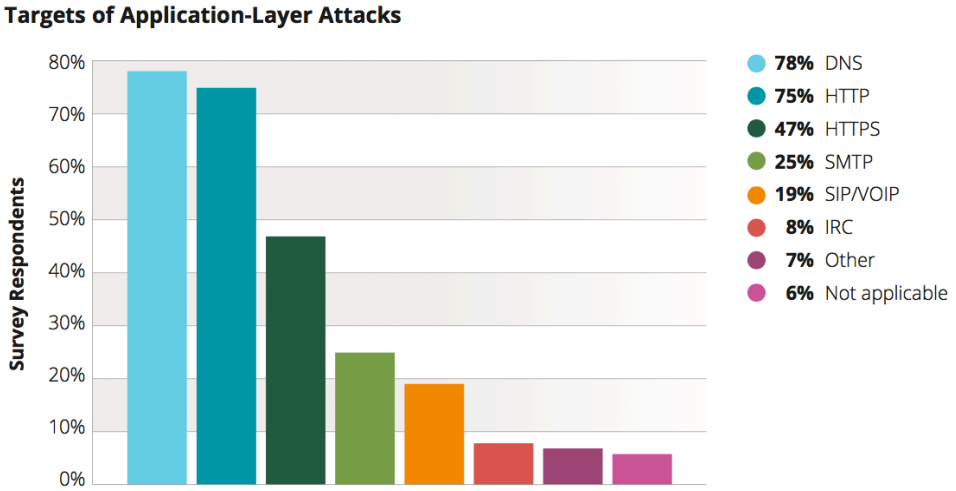

Figure 3.11: Target protocols of Application Layer attacks (Arbor Networks, 2016)

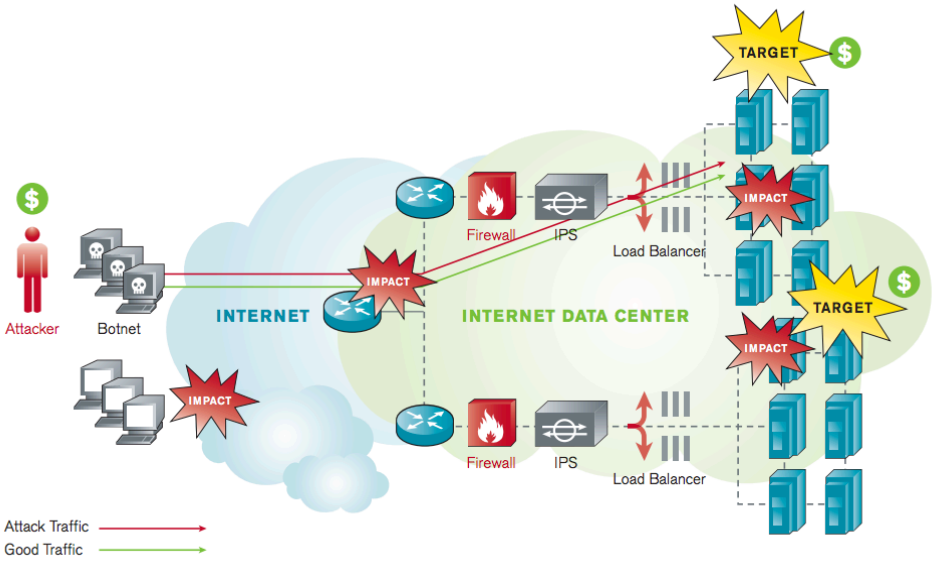

Figure 3.12: An example of application layer attack architecture (Arbor Networks, 2012)

In application layer attacks, IP packet spoofing is not used on the network layer and TCP connections are established with a target like legitimate system users do. When the connection is established successfully, attackers start to consume the resources of the target by numerous CPU intensive requests such as heavy downloading tasks (Suryawanshi and Todmal, 2015). As a result of these malicious requests, the server becomes overloaded and could not process legitimate users' requests. Malicious requests of attackers seem authenticated, and attack traffic can not be separated from legitimate traffic; thus, it is highly challenging to detect and mitigate application layer attacks. Traditional DDoS defence mechanisms are insufficient to determine and mitigate destructive application layer attacks; therefore, researchers and security analysts have recently proposed new strategies in order to detect and mitigate these types of DDoS attacks (Suryawanshi and Todmal, 2015).

Application layer DDoS attacks are becoming more sophisticated because several vulnerabilities exist in web applications and these vulnerabilities are unknown to current DDoS defence and mitigation solutions. Additionally, application development has started to move to the cloud platforms and defending against application layer attacks will probably continue to be extremely challenging. Therefore, to defend against application layer DDoS attacks, software developers should analyse the most critical web application security risks and implement their security countermeasures in the software development lifecycle. Moreover, to provide a complete defence strategy, custom DDoS security appliances should be used according to the system architecture of companies/governments.

Application layer attacks require relatively fewer system resources and these attacks are typically performed for specific aims such as preventing access to databases and interrupting transactions (Kumar, 2014). Application layer DDoS attacks are growing rapidly and more destructive than other OSI layer attacks due to the following risks and problems:

- These types of attacks use legitimate connections; therefore, it is extremely challenging to distinguish malicious requests from legitimate ones.
- A small number of TCP or UDP connections are sufficient to carry out devastating application layer attacks.
- These attacks have the ability to affect several applications. Most of them exploit HTTP, HTTPS and DNS protocol to consume the resources of the target.

- Attackers have the ability to exploit the structure of the application layer. For instance, if huge numbers of users refresh their browsers at the same time, the target may slow down and crash quickly.
- Several victims may be simultaneously affected both directly and indirectly by application layer attacks.
- Limited sources are sufficient to launch application layer attacks; therefore, attackers can conduct destructive attacks with limited opportunities.
- Malicious attack traffic could not be distinguished from normal traffic because it accomplishes every procedure required to be legitimate.
- Application layer attacks are well planned and highly targeted. Typically, these attacks are initiated to exploit specific applications (Kumar, 2014).
- Firewalls and other security devices are typically configured to allow legitimate traffic such as HTTP and DNS traffic between applications and clients; therefore, attackers eliminate one security layer easily (Arbor Networks, 2012).

3.4 Summary

In this chapter, DDoS attack types are classified based on the exploited vulnerabilities, the OSI (Open Systems Interconnection) layers and their communication methods. Moreover, DDoS attack types are explained comprehensively to show how they are initiated by attackers. It is quite challenging to examine and cope with DDoS attacks because of their distributed structure and diversity. Additionally, IP spoofing method is commonly used by DDoS attackers to change the source IP address of the malicious network packets. Attackers typically generate network packets with spoofed IP addresses to perform their malicious activities anonymously; therefore, analysing DDoS attacks becomes extremely challenging. In application layer attacks, it is quite difficult to distinguish malicious network traffic from innocent network traffic because application layer attacks use legitimate connections. Thus, analysing application layer attacks is more difficult than analysing network/transport layer attacks.

Chapter 4

Botnet-Based DDoS Attacks and Attack Trends in 2016

This chapter firstly provides extensive information about botnets and how they are used to launch destructive DDoS attacks. Subsequently, botnet control and command architectures are explained comprehensively. Finally, most recent trends in conducting botnet-based DDoS attacks are examined in detail.

4.1 Botnet-Based Distributed Denial of Service (DDoS) Attacks

Botnets are networks composed of malware compromised devices such as computers and smart phones (Silva et al., 2013). Such networks are created and managed remotely by cyber criminals in order to carry out harmful activities such as massive distributed denial of service (DDoS) attacks and phishing attacks (Silva et al., 2013; Karasaridis et al., 2007). Botnet based DDoS attack types provide the ability to slow down or crash the critical services of nations and corporations (Silva et al., 2013). The significance of the botnet mechanism is the capacity to provide anonymity with the help of control and command (C&C) structure (Feily et al., 2009). Furthermore, malware compromised devices (bot) in a botnet network can be positioned in different places around the world and these compromised devices are not actually possessed by the cyber criminals (Feily et al., 2009). Different countries have their own laws, languages and time zones; therefore, it is extremely difficult to examine botnet based DDoS attacks and determine the whole structure

of these types of attacks. Botnet based DDoS attacks which are initiated by using large numbers of bots have the ability to generate massive volumes of network traffic; therefore, these attacks become more devastating day by day (Zargar et al., 2013). Furthermore, according to a research study which was conducted in 2008, malware compromised hosts form 40% of the hosts connected to the internet in that year (Yeshwantrao and Jadhav, 2014). Therefore, these circumstances and trends make the botnet mechanism one of the most crucial risks for the cyber security of critical infrastructures (Tyagi and Aghila, 2011). Typically, a group of computers that are remotely managed by a criminal form a malicious botnet (Zargar et al., 2013). Elements of a malicious botnet and a botnet based DDoS attack example are illustrated below in Figure 4.1.

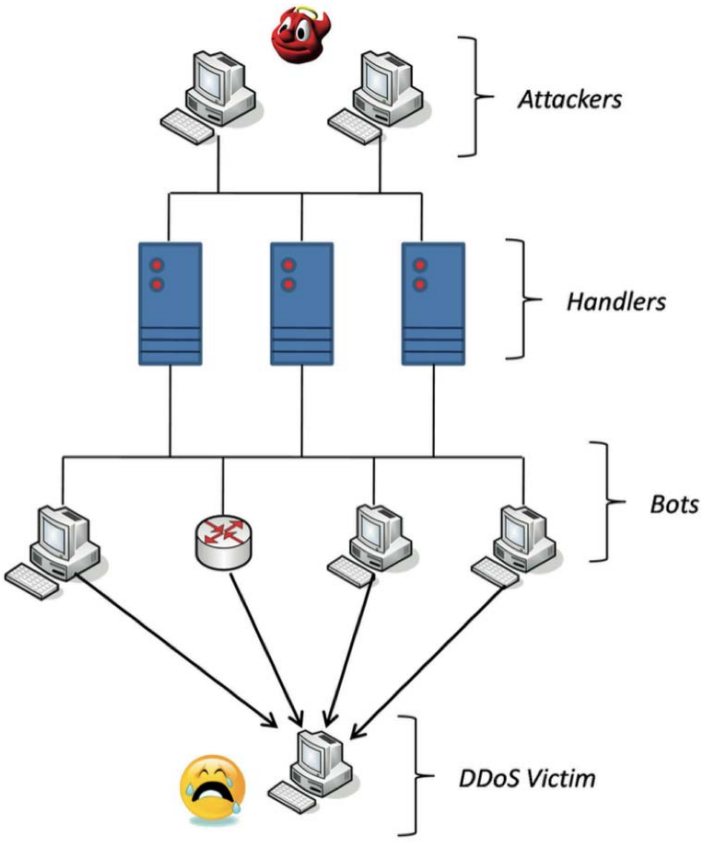

Figure 4.1: A Botnet based DDoS attack example and its elements. (Zargar et al., 2013)

A botnet consists of attackers, botnet controllers (handlers), compromised hosts (bots) and a victim (Hoque et al., 2015). The definition of botnet elements is briefly presented below.

- Attackers: The attacker control and manage the compromised hosts (bots) to launch a botnet based DDoS attack. Initially, the attacker compromises a vulnerable host to execute a malicious program and takes control of the vulnerable host once the host is infected (Hoque et al., 2015).
- Botnet Controller (Handler): Handlers send commands to the connected bots and receive messages from the connected bots in order to control them and conduct attacks (Hoque et al., 2015).
- Compromised Host (Bot): Once a host is infected with a malicious program, it becomes a bot and can be controlled by handlers (Hoque et al., 2015).
- Victim: These systems are the target of attackers that receive massive amounts of network packets from the bots of a botnet (Hoque et al., 2015).

Attackers use botnet controllers to communicate with the bots of a botnet indirectly. However, malicious programs which are installed on compromised hosts leave identifiable footprints and these footprints can be detected with modern antivirus programs (Zargar et al., 2013). Therefore, attackers recently use alternative communication mechanisms, such as Internet Relay Chat (IRC), in order to control and update their bots.

4.2 Architectural Designs of Botnet Control and Command (C&C) Mechanisms

Analysing and determining the control and command (C&C) architecture of botnet based DDoS attacks plays a crucial role in mitigating these type of attacks. C&C architectures are basically divided into four categories. These architectures are centralized, decentralized, random and hybrid architecture (Hoque et al., 2015). Centralized, decentralized and hybrid C&C architectures are illustrated respectively below in Figure 4.2(a), Figure 4.2(b) and Figure 4.2(c).

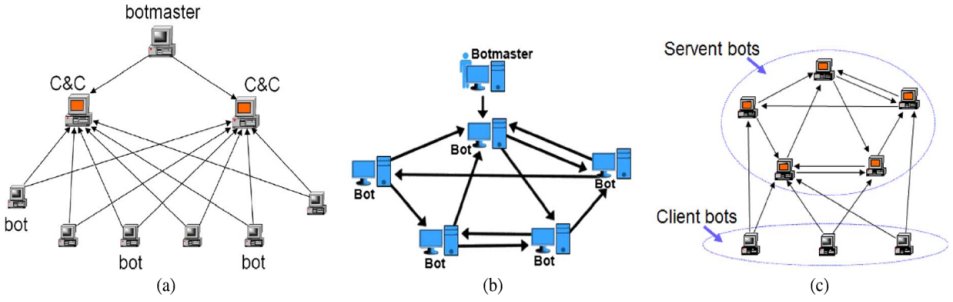

Figure 4.2: Botnet C&C architectures. (a) centralized (b) decentralized (c)hybrid (Hoque et al., 2015)

4.2.1 Centralized C&C Architecture

The centralized control and command (C&C) architecture is identical to the typical client/server network architecture (Silva et al., 2013). The most common models of centralized C&C architecture are those established using the IRC (Internet Relay Chat) protocol. In a centralized architecture, each bot establishes its own communication link with one or more connection points. These points are generally control and command (C&C) servers which are used by a botmaster in order to control and update its bots. The benefits of centralized C&C architecture are perfect coordination and fast response time (Silva et al., 2013). Moreover, it provides anonymous, low latency and powerful real-time mechanism for botnet based DDoS attacks (Hoque et al., 2015). In spite of its huge benefits, centralized C&C architecture also has some limitations. C&C servers have a central point of failure risk; therefore, operations of a discovered botnet can be aborted easily (Silva et al., 2013). Furthermore, if the C&C server could not continue to perform its operations, the botnet also could not continue to carry out DDoS attacks because none of its bots can get commands and updates which are necessary to perform their tasks (Hoque et al., 2015). The major communication protocols used in establishing centralized C&C architecture are HTTP (Hypertext Transfer Protocol) and IRC (Internet Relay Chat).

- IRC Based Architecture: IRC protocol is a text-based communication mechanism used for instant messaging between users, and this protocol has the capability to connect hundreds of users by several IRC servers (Zargar et al., 2013). In IRC based botnets, attackers create IRC channels as botnet controllers and use these channels in order to send instructions to the bots and conduct malicious activities such as botnet based DDoS attacks (Zargar et al., 2013; Silva et al., 2013). Analysing and determining the DDoS attack structure becomes extremely difficult when IRC protocol is used over legitimate ports. Moreover, attackers can conceal their malicious activities easily due to the vast volumes of message traffic generated by IRC servers (Zargar et al., 2013). Furthermore, attackers can distribute harmful files via IRC channels in order to execute their malicious codes on the bots of their botnets. Additionally, attackers do not need to keep the list of their bots locally because they can see their bots list by connecting to the IRC channels. However, the IRC protocol has critical weaknesses because detecting an IRC botnet and terminating its operations are quite easy (Silva et al.,

2013). Therefore, the whole botnet mechanism can be halted by blocking the IRC traffic with firewalls if the target detects the C&C servers.

- HTTP Based Architecture: Attackers have currently started to use HTTP protocol for establishing centralized C&C communication because most networks started to block IRC traffic (Silva et al., 2013; Zargar et al., 2013). In HTTP based architecture, botnets do not establish connections like they do in IRC based architecture. Instead, the bots of an HTTP botnet get commands using HTTP requests (Zargar et al., 2013). Botnets are controlled and updated via advanced scripts, and encrypted communication is provided over HTTPS or HTTP protocol by these scripts. Therefore, analysing HTTP based C&C architecture is more difficult that analysing IRC based C&C architecture (Zargar et al., 2013). However, HTTP based architecture has also a central point of failure vulnerability because of its centralized architecture (Silva et al., 2013).

4.2.2 Decentralized C&C Architecture

Attackers try to find out advanced botnet communication structures, which have the capability to provide excellent durability and higher flexibility in malicious activities, in order to increase their profits and control huge numbers of bots (Silva et al., 2013). In decentralized C&C architecture, the detection of several bots in a botnet does not lead to the failure of a botnet mechanism because decentralized architectures do not have any central C&C server that can be discovered and stopped. Therefore, it is extremely difficult to reveal the whole structure of botnets which have decentralized C&C architectures and prevent the activities of these types of botnet communication architectures. Decentralized C&C architecture is generally based on types of P2P (Peer to Peer) communication protocol and act as an overlay network (Silva et al., 2013). These types are Structured P2P overlays, Unstructured P2P overlays and Superpeer P2P overlays.

- P2P Based Architecture: Large numbers of people share their pictures, documents, programs, sources, computer games and movies utilizing P2P communication protocol and the popularity of this protocol has increased tremendously in recent years. Attackers started to use P2P protocol in order to distribute their malicious codes and conduct other criminal activities because of the popularity and flexibility of this protocol (Hoque et al., 2015).

In P2P architecture, each bot (peer) of the botnet works as both server and client and tries to establish a connection to the other bots (peers) of the botnet using their known peers list (Yuce, 2011). When bots receive an instruction, they forward it to the connected peers using their private peer list (Hoque et al., 2015). Bots also update their peer list in order to have an enhanced coordination (Yuce, 2011). An example of P2P architecture is illustrated below in Figure 4.3. In this example, the discovery of the botnet controller is challenging because the botnet operator works as a peer like all other bots (Yuce, 2011).

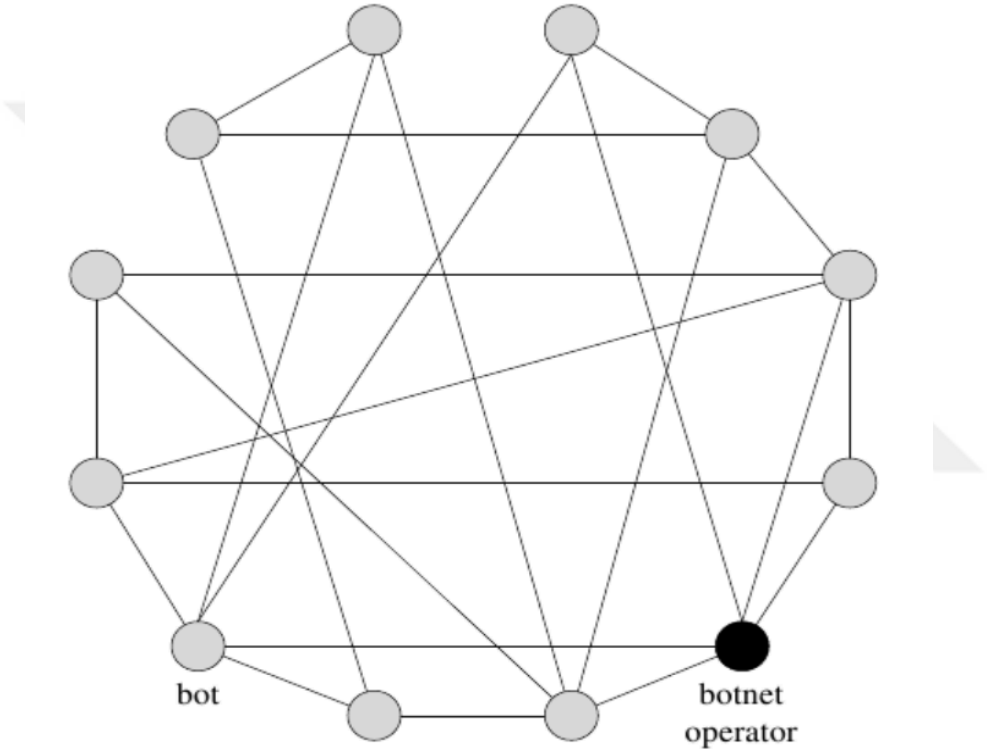

Figure 4.3: An example of P2P based architecture (Yuce, 2011)

A crucial benefit of P2P architecture is that the botnet controller can send commands over the network by connecting one of its bots because each bot regularly connects to its peers to retrieve commands from the botnet controller (Hoque et al., 2015). Moreover, P2P architecture is more powerful and durable than centralized architectures. Furthermore, their architectural design is not too complex, and it is quite challenging to examine and detect these types of designs. However, P2P based architectures do not provide a guaranteed message delivery (Hoque et al., 2015).

4.2.3 Hybrid C&C Architecture

These types of architectures are designed to use the positive aspects of both decentralized and centralized C&C architectures (Silva et al., 2013). In a hybrid botnet model, bots are separated into two groups: client bots and servant bots. Servant bots act both as servers and clients, and they have routable static IP addresses. In contrast to servant bots, client bots refuse incoming connection requests, and they have non-routable dynamic IP addresses (Wang et al., 2010). Additionally, client bots can be positioned behind firewalls without being globally connected to the Internet. All client bots should regularly communicate with the servant bots, which are recorded on their known peers list, in order to receive commands sent by their botnet controller. When client bots receive new messages, they immediately forward these messages to the servant bots which are recorded on their known peers list (Silva et al., 2013). Servant bots listen on a specific port for incoming connection requests, and a symmetric encryption key is used for communication. Therefore, analysing and determining the whole botnet structure becomes more challenging (Silva et al., 2013).

4.2.4 Random C&C Architecture

In this architecture, each compromised bot node knows only one other compromised bot node. If bots or botnet controllers try to send a message, they scan the Internet randomly in order to find another bot. When they discover a bot, they encrypt the message and sent it to the discovered bot (Cooke et al., 2005). This architecture becomes attractive because of its secure and simplified design. Moreover, the discovery of a bot is insufficient to reveal the whole botnet structure. However, this architecture does not provide a guaranteed mechanism for message distribution and has a high message latency. Furthermore, this architecture has detectability risks because of its random scanning behaviour (Cooke et al., 2005).

4.2.5 Summary and Comparison

The summary of Control and Command (C&C) architectures is illustrated below in Figure 4.4. Additionally, the weaknesses and strengths of centralized, peer-to-peer and random command and control (C&C) topologies are compared and illustrated below in Figure 4.5.

Factors	Centralized (IRC,HTTP)	Hybrid DDNS	Peer-to-Peer P2P
Detection	Easy	Medium	Hard
Resilience	Low	Fairly High	Very High
Latency	Low	Medium	Fairly Hard
Traceback	Fairly Hard	Hard	Very Hard
Complexity	Easy	High	Medium
Experience	Very High	None	Medium

Figure 4.4: The summary of Control and Command (C&C) architectures (Vania et al., 2013)

Topology	Design Complexity	Detectability	Message Latency	Survivability
Centralized	*Low*	*Medium*	*Low*	*Low*
Peer-to-Peer	*Medium*	*Low*	*Medium*	*Medium*
Random	*Low*	*High*	*High*	*High*

Figure 4.5: The weaknesses and strengths of command and control topologies (Cooke et al., 2005)

4.3 Botnet Based DDoS Attack Trends in Q1 2016

Kaspersky Lab has published DDoS Intelligence Report for the first quarter of 2016, demonstrating botnet based DDoS attack statistics. This report is based on the botnets that were discovered and examined by Kaspersky Lab. There are several mechanisms used to conduct distributed denial-of-service (DDoS) attacks. Botnets are only one of these mechanisms; therefore, all DDoS attacks occurred in the stated time interval are not included in this report. According to Kaspersky (2016), DDoS attackers target the sources of 74 countries in the first quarter of 2016 and 93.6% of the sources targeted by attackers were positioned in 10 countries. Distribution of botnet based DDoS attacks by these 10 target country is illustrated below in Figure 4.6. Additionally, the longest botnet based DDoS attack time period recorded in the first quarter of 2016 is 197 hours and the maximum number of DDoS attacks recorded in a day is 1272. Distribution of botnet based DDoS attacks by attack duration is illustrated below in Figure 4.7.

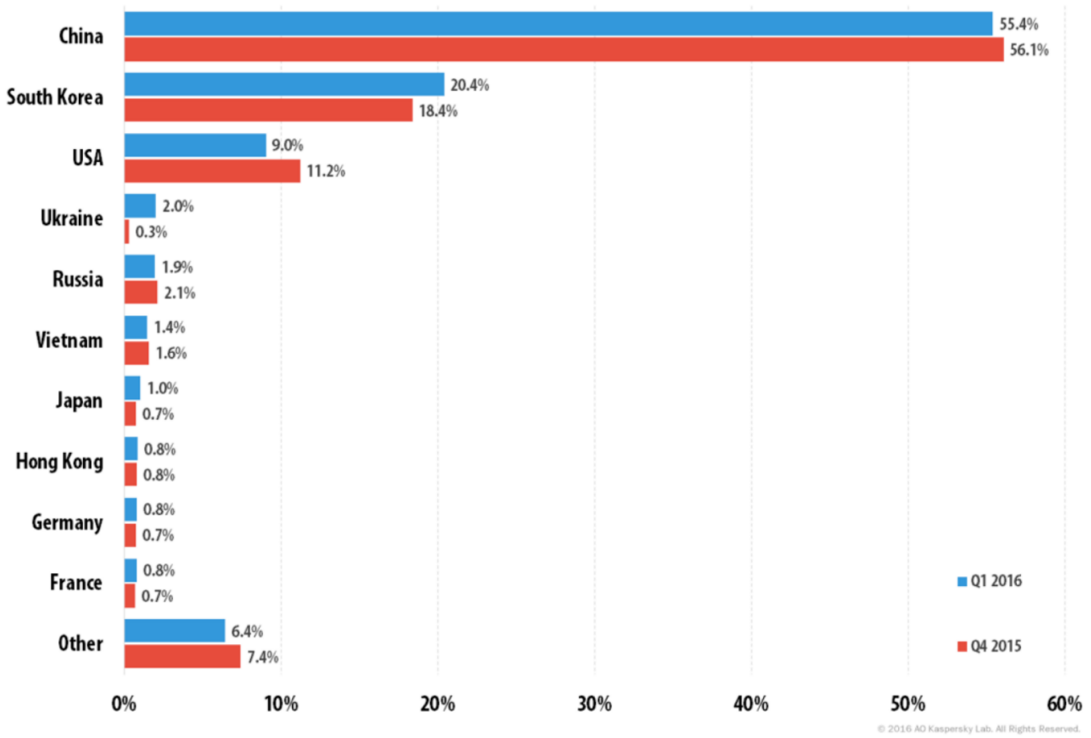

Figure 4.6: Botnet based DDoS attacks by target country, Q4 2015 vs. Q1 2016 (Kaspersky, 2016)

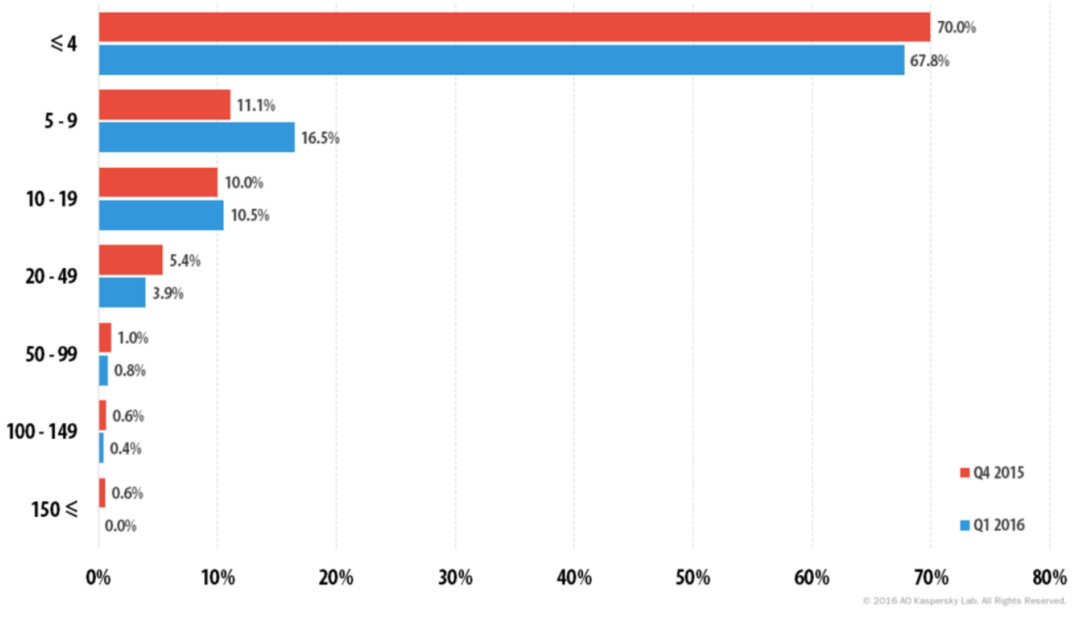

Figure 4.7: Botnet based DDoS attacks by attack duration, Q4 2015 / Q1 2016 (Kaspersky, 2016)

The most favoured types of DDoS attacks which conducted in the first quarter of 2016 are SYN DDoS, UDP DDoS, HTTP DDoS, TCP DDoS and ICMP DDoS. Distribution of botnet based DDoS attacks by these attack types is illustrated below in Figure 4.8.

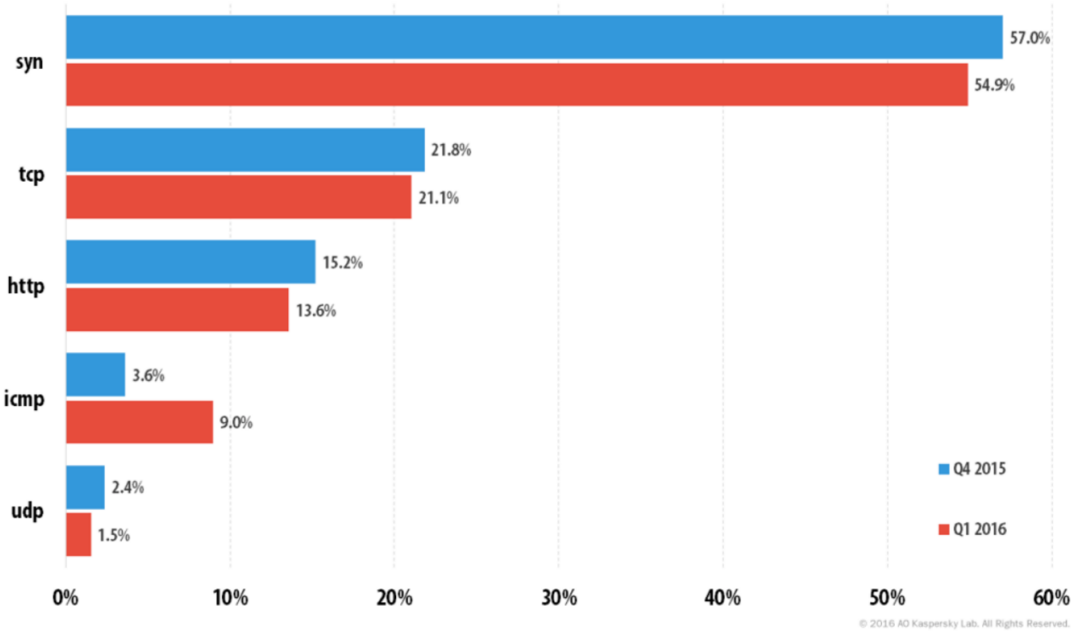

Figure 4.8: Botnet based DDoS attacks by attack type, Q4 2015 vs. Q1 2016 (Kaspersky, 2016)

Kaspersky (2016) states that current DDoS mitigation solutions are useful in dealing with network layer, data link layer and transport layer attacks. However, they expect that application layer (Layer 7) attacks and multi layer attacks (a mixture of hardware and application layer) will continue to increase. According to the statistics of Kaspersky (2016), in the first quarter of 2016, they have fought against much more HTTP and HTTPS attacks than they did during 2015. To initiate massive application layer attacks, huge botnets or several numbers of high performance servers and an immense output tunnel is needed (Kaspersky, 2016). Moreover, attackers should analyse the target and discover its vulnerabilities before launching an application layer attack. If an application layer attack is conducted in a well planned manner, it is extremely challenging to mitigate it without preventing legitimate users' traffic because harmful requests seem authenticated and each bot accomplishes the connection procedure successfully (Kaspersky, 2016). Huge numbers of service requests are the only abnormality. The cost of performing a devastating application layer attack is decreasing due to large numbers of configuration weaknesses at the application layer and the increase in compromised

devices and computers (Kaspersky, 2016). Therefore, more efficient defence strategies should be developed to guarantee application layer attacks are economically unattractive for the attackers.

Additionally, 99.73% of DDoS attacks in the first quarter of 2016 were initiated by bots using the same operating system family. Attackers have the ability to initiate DDoS attacks from both Linux and Windows botnets. In the fourth quarter of 2015, Windows botnets and Linux botnets constitute respectively 45.2% and 54.8% of total botnets. However, in the first quarter of 2016, Windows botnets and Linux botnets constitute respectively 55.5% and 45.5% of total botnets. As mentioned in botnet C&C architectures part, C&C servers have a crucial role in botnet based DDoS attacks. Distribution of botnet command and control (C&C) servers by country is illustrated below in Figure 4.9. This information can be used in order to mitigate botnet based DDoS attacks or develop more effective defence mechanisms.

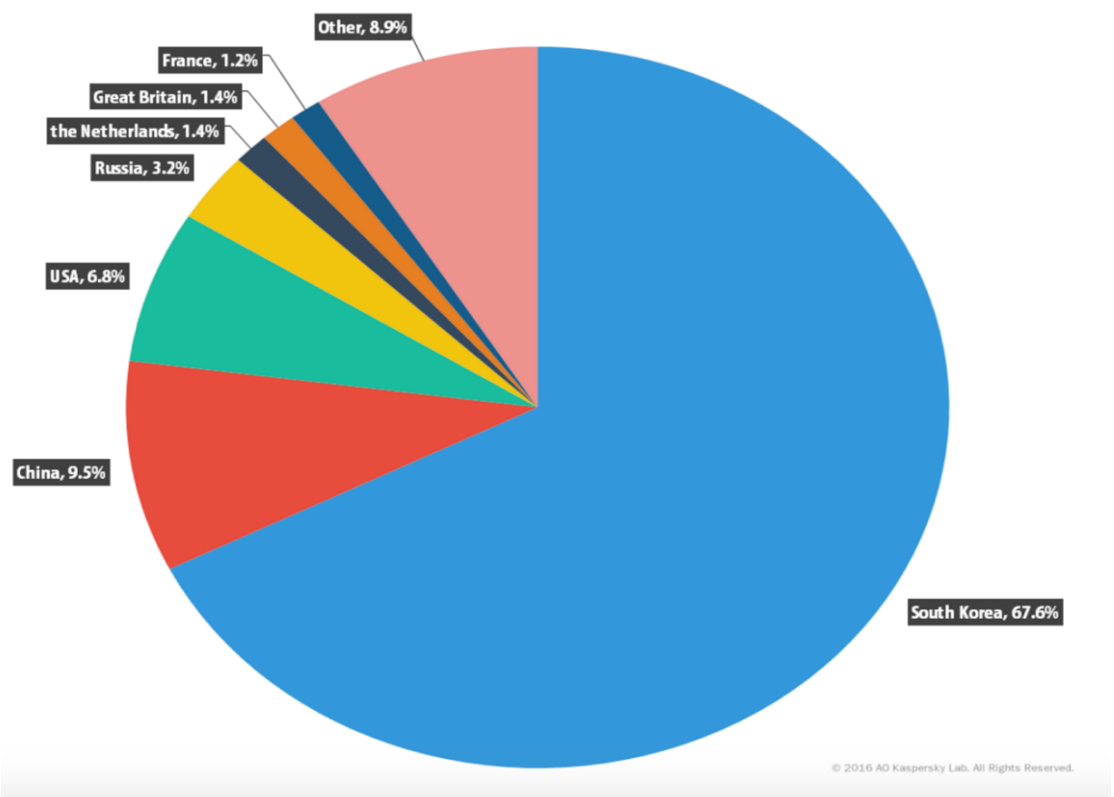

Figure 4.9: Distribution of botnet command and control servers by country (Kaspersky, 2016)

4.4 Summary

In this chapter, botnets and the architectural designs of their control and command (C&C) mechanisms are explained extensively. Furthermore, the trends of DDoS attacks that use botnets are analysed to reveal most preferred DDoS attack types. Botnets play a critical role in conducting devastating DDoS attacks. Attackers have the ability to control their bots using harmful programs that are set up on these compromised hosts. However, advanced anti-virus programs can discover these harmful programs. Therefore, attackers have started to utilise from internet protocols such as P2P, IRC and HTTP(S) to communicate with their botnets and manage them.

TCP, HTTP(S), DNS, UDP and ICMP protocols are frequently exploited to initiate massive DDoS attacks. Additionally, it is expected that the number and impact of application layer attacks will increase in the next years.

Chapter 5

Botnet-Based DDoS Attacks Detection Methods and Mitigation Mechanisms

This chapter presents comprehensive information about botnet-based DDoS attack mitigation and detection techniques. It firstly provides detailed information about anomaly-based and signature-based detection methods. Afterwards, these detection methods are compared to discover their drawbacks and strengths. Finally, some of the most preferred DDoS mitigation solutions are explained to reveal their benefits and limitations.

5.1 Classification & Comparison of Botnet Based DDoS Attacks Detection Methods

Botnet based DDoS attack detection methods are basically separated into two types: anomaly-based detection and signature-based detection (Alomari et al., 2016). Each detection method has its unique drawbacks and benefits. The advantages and shortcomings of these detection methods are analysed and compared below.

5.1.1 Signature-Based DDoS Attack Detection Method

In this detection method, network traffic is captured by network monitoring tools and compared with well-known and destructive attack models (Douligeris and Mitrokotsa, 2004). Signature-based detection method can be utilized to extract and analyse the handler/agent communication; however, this method becomes useless if encryption techniques are used to protect the handler/agent communication (Shameli-Sendi et al., 2015). Most of the DDoS attack detection methods are signature-based, and signature-based detection methods behave like an antivirus software. They try to discover the signature or characteristic of each distinct type of DDoS attack traffic (Alomari et al., 2016).

Signature-based DDoS attack detection methods are highly effective in determining well-known DDoS attacks; however, their effectiveness is highly dependent on updating signature records periodically (Patcha and Park, 2007). Therefore, a signature-based DDoS attack detection technique can only be as powerful as its signature database. The discovery of DDoS attack signatures requires analysing network traffic to find packet or byte series that are noted to be harmful. A well-defined signature should frequently appear in the DDoS attack traffic. Additionally, it should barely appear in the legitimate traffic (Tang and Chen, 2005). The main strength of signature-based detection method is that well-known DDoS attacks can easily be detected. However, these types of detection methods can only discover well-known attacks if their signatures are revealed by network analysts. The creation of attack signatures is quite challenging because of three main reasons. Firstly, to create a signature, attack traffic should be identified and distinguished from the normal network traffic. Secondly, the signature which will be created should have the capability to capture whole attack traffic of a certain DDoS attack and allow legitimate traffic to prevent unwanted conditions. Finally, generated detection method should be adaptable to cope with the different variations of the target DDoS attack traffic (Tang and Chen, 2005).

5.1.2 Anomaly-Based DDoS Attack Detection Method

In a computer network, exceptional traffic patterns generated by internal or external entities are called anomalies (Karim et al., 2014). Anomaly-based DDoS attack detection methods try to find abnormal network traffic that does not match up with the expected network traffic behaviour. The main aim of these detection methods is to identify expected network traffic behaviour and discover any

malicious deviation from the identified behaviour (Chen et al., 2007). Expected behaviour of the system can be determined by using the following techniques:

- Making comparisons between reverse and forward network traffic: In this technique, incoming network traffic and outgoing network traffic is calculated systematically, and this two calculated traffic should be proportional to each other. If there is no direct proportion between this two traffic, this can be explained as a repetitive downloading of huge files. The weakness of this technique is that attacks which use legitimate traffic could not be discovered (Shameli-Sendi et al., 2015).

- Detecting abnormal behaviour with the statistics of connections: The number of established connections, the life span of the sessions and the count of created sessions can be used to discover abnormal behaviours. For instance, the statistics of TCP sessions can be tracked and utilized to determine exceptional behaviours.

- Observing the behaviour of aggregate traffic: The incoming network traffic and outgoing network traffic is separated into particular network traffic aggregates and examined to discover patterns. The observed traffic type should have the same characteristics such as HTTP and UDP connection.

- Observing the behaviour of flow traffic: The flow traffic of the network is observed in order to control different flow types. Machine learning is utilized to determine the expected behaviour of the network and discover the exceptional behaviours (Shameli-Sendi et al., 2015).

In anomaly-based detection methods, alerts are generated by any abnormal traffic behaviour that does not match up with the predetermined or expected traffic behaviour patterns (Alomari et al., 2016). Anomaly-based detection methods work by observing the exceptional activities in each part of the system and making comparisons between the normal behaviour and the observed behaviour (Pimentel et al., 2014). The observed exceptional behaviours that surpass the determined thresholds for the anomalies are called as malicious activities. The complexity of determining the standard rules is one of the drawbacks of the anomaly-based detection systems (Owezarski, 2009). The rule-determining procedure is also influenced by the collections of protocols that utilized by different information technology companies. Furthermore, determining the standard rules becomes also extremely challenging because of custom protocols. In order to detect anomalies properly,

administrators should provide quite detailed information about the expected behaviour of each part of the system. Once the standard rules are determined and the required solution is designed, the anomaly-based detection method will begin to operate effectively. However, if a harmful activity could not be detected with the determined parameters of the expected behaviour, it will be accepted as a legitimate activity. Signature-based detection methods could not detect attacks without having their signatures. Therefore, signature-based methods could not discover new attack types that are exploiting zero-day vulnerabilities. However, anomaly-based detection methods have the ability to detect new attack types if these attacks are accepted as exceptional system behaviour (Alomari et al., 2016). The advantages of this characteristic can be easily seen when an anomaly-based detection method discovers a new type of worm. When a new type of worm infects a vulnerable host, it commonly tries to discover other vulnerable hosts on the network and begins flooding the infected network with harmful traffic. The weaknesses and strengths of anomaly-based DDoS attack detection methods and signature-based DDoS detection methods are compared and illustrated below in Figure 5.1.

Signature-based Detection	Easy to develop and understand by matching whole string	Cannot identify the new behaviours
Anomaly-based Detection	Indentify the anomalies by predefined or accepted behavioural model	Difficulty in defining the rule set, high false positive

Figure 5.1: The weaknesses and strengths of anomaly-based and signature-based detection methods (Alomari et al., 2016)

5.2 Botnet-Based DDoS Attack Mitigation Mechanisms

A DDoS mitigation technique is performed on a specific component of the system as a local countermeasure; however, a DDoS mitigation strategy aims to deploy several countermeasures at different parts of the system in order to cope with massive DDoS attacks (Shameli-Sendi et al., 2015). In the following part, some of the most important DDoS mitigation techniques and strategies are explained in the light of the proposed solutions that target to mitigate botnet based massive DDoS attacks. Moreover, the benefits and limitations of these mitigation techniques and strategies are also explained. Additionally, comparisons are made between them in order to show their weaknesses and strengths.

5.2.1 DDoS Mitigation Techniques

5.2.1.1 Ingress/egress filtering

Ingress filtering is defined as filtering the incoming network traffic, while egress filtering is defined as filtering the outgoing network traffic (Beitollahi and Deconinck, 2012). A study of Ferguson and Senie (2000), RFC 2827, is used in order to explain ingress/egress filtering procedure in Figure 5.2. As illustrated in Figure 5.2, internet service provider which is named ISP D provides services to the network A for accessing the internet. Router 2 and Router 3 are the edge routers of ISP D and the name of the edge router of the network A is router 1. In this figure, ISP D also provides the address scope of 204.69.207.0/24 to the network A. Additionally, attacker X is located in the network A, while attacker Y is located in another network which has a connection to the ISP D. ISP D can create an ingress filter and set up this filter on router 2's input port. In this way, the created filter drops any network packet which is sent from the network A with an IP address outside the scope of 204.69.207.0/24. Therefore, if attacker X creates network packets with spoofed IP addresses outside the address scope of 204.69.207.0/24 and sends them, these spoofed packets will be dropped by the router 2's ingress filter (Beitollahi and Deconinck, 2012). Correspondingly, the network A can create an egress filter and set up it on router 1's output port. In this way, the created filter can drop any network packet which is created with spoofed IP addresses outside the address scope of 204.69.207.0/24 before network packets leave the network A (Beitollahi and Deconinck, 2012).

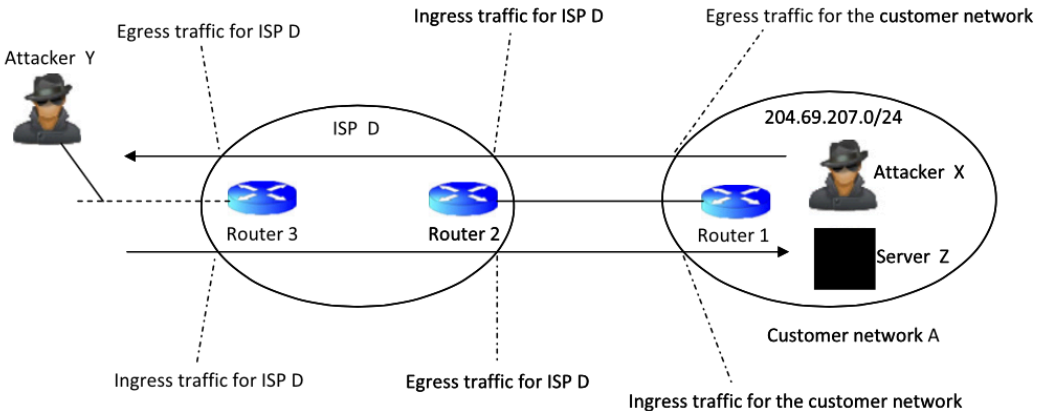

Figure 5.2: An ingress filtering example according to RFC 2827 (Beitollahi and Deconinck, 2012)

Additionally, ISP D can create an ingress filter and set up this filter on router 3's input port. In this way, the created filter drops any network packet which is coming with spoofed source IP address. Therefore, if attacker Y creates network packets with spoofed IP addresses such as 200.*.*.* and sends them, these spoofed packets will be dropped by the router 3's ingress filter. Correspondingly, ISP D can create an egress filter and set up it on router 2's output port. In this way, the created filter can drop any network packet which is created with spoofed IP addresses before network packets leave the ISP D. As a result of the created egress filter on router 2's output port, any network packet which is created with spoofed IP addresses does not forwarded to the edge router (router 1) of network A. Filtering which is done by ingress filters is named as ingress filtering, while filtering which is done by egress filters is named as egress filtering (Beitollahi and Deconinck, 2012).

Ingress/egress filtering has some limitations due to the following challenges:

1. Ingress/egress filtering technique can be successful in mitigating DDoS attacks only if almost all of the ISPs implement ingress/egress filters. If attackers detect the ISPs which do not have any ingress/egress filtering mechanism, they can use the compromised hosts of these detected ISPs in order to launch DDoS attacks (Beitollahi and Deconinck, 2012).

2. Attackers can still create network packets with spoofed IP addresses if the spoofed IP address is chosen from the attacker's sub-network range. For instance, in Figure 5.2, if attacker X create network packets with spoofed IP addresses chosen from the 204.69.207.x network, router 2's ingress filter could not detect these spoofed network packets.

3. Recently, most of the devastating DDoS attacks use botnets, and attackers do not require any protection mechanism to hide the compromised hosts of a botnet. By exploiting huge numbers of compromised hosts, attackers can initiate several types of DDoS attacks without utilizing IP address spoofing. For example, the compromised hosts of a botnet do not use spoofed IP addresses to carry out HTTP flood DDoS attacks. In this situation, Ingress/egress filtering technique could not be effective in mitigating destructive DDoS attacks.

4. Filters should be maintained regularly after the installation procedure is accomplished. Therefore, administrative expenses increase due to the installation and maintenance process. Moreover, ingress/egress filtering technique does not provide any advantage to the ISPs.

5. In ingress/egress filtering, routers which are implementing the filters have to control and apply new rules for each network packet. Therefore, filtering process may increase performance costs. In most of the circumstances, ingress/egress filtering technique can control network packets utilizing a small number of rules without considerably affecting the performance of routers. However, this could not be accomplished in every network. This technique may result in a remarkable decrease in the performance of routers that provide service to huge numbers of various address ranges. In this situation, those routers have to be changed with powerful ones in order to prevent performance problems and continue serving customers (Beitollahi and Deconinck, 2012).

Ingress/egress filtering technique is not a powerful mechanism against botnet based DDoS attacks because of these crucial challenges. Furthermore, the administrators of ISPs are doubtful about installing filters at ISP's customer edge routers (Beitollahi and Deconinck, 2012).

5.2.1.2 Rate limiting

The Rate-limiting technique is broadly used in mitigating massive DDoS attacks, and it is accepted as one of the most effective DDoS mitigation techniques. This technique achieves its aim by rejecting a part of the incoming network traffic (Shameli-Sendi et al., 2015). Rate-limiting can be separated into two groups: flow rate-limiting and aggregate rate-limiting.

1. **Flow rate-limiting:** This type of rate-limiting provides an effective policing mechanism to routers in order to manage network traffic congestion (Chen et al., 2004). In this technique, the typical features of the network traffic flow are determined by identification algorithms. Once the features are discovered, flow rate-limiting restricts the network flow transmission rate below the calculated rate. Therefore, network packets transmitted at a higher rate are dropped or discarded at the routers (Chen et al., 2004).

2. **Aggregate rate-limiting:** This technique aims to decrease DDoS attack traffic by limiting the consumption of the network bandwidth required for aggregate traffic (Shameli-Sendi et al., 2015). Several criteria, such as destination address and application traffic type, are used to define aggregate traffic. For example, the details in the IP packet header or network traffic

analysis can be used in order to define the application traffic type and aggregate traffic. Then, application traffic surpassing the determined level can be limited by aggregate rate-limiting (Shameli-Sendi et al., 2015).

Both rate-limiting and IP packet filtering are mitigation techniques to defend against botnet based DDoS attacks; however, they try to mitigate massive DDoS attacks and restrict malicious traffic in different ways (Chen et al., 2004). IP packet filtering rejects any IP packet that matches up with the typical features of DDoS attack traffic. However, rate-limiting could not prevent the flow of a part of DDoS attack traffic, but this malicious flow is restricted by a network flow transmission rate. Therefore, packet filtering can be successful in mitigating DDoS attacks only if it is used with DDoS attack detection methods such as anomaly-based detection, and rate-limiting is commonly preferred when the malicious network traffic could not be distinguished from normal network traffic (Chen et al., 2004).

5.2.1.3 DDoS Network Attack Recognition and Defence (D-WARD)

D-WARD is one of the DDoS defence mechanisms that is set up at the gateways/routers of the source-end networks. The aim of D-WARD is to discover and stop outgoing massive DDoS attacks by examining outgoing network traffic while allowing the flow of legitimate network traffic (Mirkovic and Reiher, 2005). In the autonomous implementation, D-WARD mechanism tries to discover DDoS attacks and prevent them without receiving any support from other system entities. However, in the distributed collaborative implementation, the detection mechanism of D-WARD is improved by receiving DDoS attack warnings from other system entities. It is presumed that D-WARD has the ability to examine each IP packet transferred between the internet and the source network. The design of D-WARD is constituted by traffic-policing units, rate-limiting and observation. In the observation process, each IP packet passing through the gateway/router of the source network is monitored and the statistics of the network traffic is collected. Additionally, these statistics are regularly compared with legitimate network traffic examples and network traffic is categorized as legitimate traffic or attack traffic (Mirkovic and Reiher, 2005). After this gathered information is evaluated, the observation unit sends evaluated information to the rate-limiting unit. Then, D-WARD executes a rate-limiting process to every suspicious outgoing network traffic in order to slow down or stop potential DDoS attack attempts (Mirkovic and Reiher, 2005). D-WARD has the capability to mitigate DDoS attacks that use ICMP, UDP and TCP protocols. These protocols are commonly utilized in

launching DDoS attacks. However, other internet protocols, such as DNS and NTP, become widely used over the internet. Therefore, D-WARD needs to be enhanced in order to mitigate the different types of DDoS attacks (Mirkovic and Reiher, 2005). D-WARD also has the capability to easily discover DDoS attacks that cause anomalies in the network traffic (Beitollahi and Deconinck, 2012). Additionally, it reduces the severity of massive DDoS attacks at the network which the attack originated from. Therefore, the negative effects of DDoS attacks become limited on the target (Beitollahi and Deconinck, 2012). However, D-WARD technique has some limitations due to the following challenges:

1. The D-WARD technique can efficiently mitigate botnet based DDoS attacks only if this technique is broadly installed on the internet by ISPs. However, this could not be entirely achieved and seems improbable.

2. Deploying D-WARD does not provide any advantage to the ISPs. Therefore, deploying D-WARD on edge routers is not popular and widespread among the administrators of ISPs.

3. D-WARD technique regulates the network flow and set policies to stop outgoing destructive DDoS attacks. Therefore, D-WARD technique considerably reduces the performance of the network systems. Additionally, D-WARD slows down the internet connection of the systems that use D-WARD filters. Therefore, the users of these systems could not use the internet with high speed (Beitollahi and Deconinck, 2012).

4. D-WARD generates additional works and costs to the border routers because they have to continuously monitor network traffic and categorize network traffic according to destination IP addresses. Moreover, these routers have to calculate the statistics for each category and make comparisons between the calculated statistics and known attack models. Then, rate-limiting is applied to each category according to the comparisons. Additionally, routers should have adequate resources, such as memory and processing unit, in order to perform their tasks. Therefore, routers need to be enhanced with adequate resources. However, installing D-WARD does not provide any advantage to the ISPs; thus, the administrators of ISPs are reluctant to allocate budget for those powerful routers.

5. Discovering DDoS attack traffic in the source network, without restricting legitimate network traffic, is extremely challenging. Additionally, D-WARD is

not a highly efficient mechanism against application layer attacks (Beitollahi and Deconinck, 2012).

It can be concluded that the administrators of ISPs are reluctant to set up D-WARD filters on the edge routers because of these challenges. Moreover, each user of an ISP could not use the internet with high speed due to a potential attack against a target positioned in other ISPs. Additionally, D-WARD should continuously analyse network traffic even if there is no malicious activity against a target. Because of this, the users of the ISP may encounter performance problems when D-WARD performs its tasks (Beitollahi and Deconinck, 2012).

5.3 DDoS Mitigation Strategies

5.3.1 Collaborative Strategy

Collaborative mitigation strategies can be classified as Blackholing, Pushback and Firewall cooperative defence based on the type of collaboration and the security architecture of the network (Shameli-Sendi et al., 2015).

5.3.1.1 Firewall Cooperative Defence

In this type of strategy, several firewalls that communicate with each other are located in the network. Moreover, they collaborate together in order to block or mitigate DDoS attacks at the nearest appropriate firewall unit (Shameli-Sendi et al., 2015). Additionally, each firewall unit has the ability to declare its security policies by broadcasting them to the other firewalls in the network. For example, a cooperative defence firewall protocol for classic networks was proposed by El-Soudani and Eissa (2003). In this protocol, firewalls are separated into two groups: Assistant Firewall (AFW) and Defender Firewall (DFW). A Defender Firewall examines each incoming network packet using its database that holds security policies. If a security breach is detected, the Defender Firewall creates a broadcast message in order to transmit its security policies. The aim of creating a broadcast message is to block the attacker as early as possible. When the broadcast message is received by assistant firewalls, they analyse the security policies included in the broadcast message and insert these policies into their local security policy databases (El-Soudani and Eissa, 2003).

5.3.1.2 Pushback Cooperative Defence

In pushback cooperative defence strategy, routers collaborate together to mitigate or prevent DDoS attacks (Shameli-Sendi et al., 2015). 'Pushback' terminology is used to describe the fact that a network unit or security device pushes the detailed information about the DDoS attack traffic to all other network or security units. The receiving units are normally located in front of the originator of the harmful attack traffic on the transmission route to the victim (Chen et al., 2004). The details of congestion, such as expiration time, network bandwidth limit and signature, are transmitted to the upstream router to apply rate-limiting techniques to the DDoS attack traffic as soon as possible.

Pushback, which is the first cooperative defence strategy, can efficiently provides protection against massive DDoS attacks when the botnets and compromised hosts of attackers are located in few points (Beitollahi and Deconinck, 2012). If attacker's botnets or compromised hosts are broadly distributed all over the world, legitimate users' traffic is also blocked by rate-limiting techniques and pushback strategy could not be highly successful. Therefore, pushback defence strategy potentially punishes legitimate users' traffic. Moreover, this strategy also potentially blocks legitimate resources that use the same routes with the malicious resources. Additionally, each router between the source of DDoS attack traffic and the congested routers is included in the pushback process; thus, the cost of this defence strategy is too high (Beitollahi and Deconinck, 2012). Furthermore, each router should periodically analyse traffic flows and communicate with its downstream routers to notify them of the results of the analysis. Therefore, each router in the pushback cooperative defence strategy requires sufficient memory and processing power. DDoS attacks have the ability to target several servers at the same time. In this situation, if the pushback messages could not be received by the upstream routers, this strategy could not protect the target servers efficiently (Beitollahi and Deconinck, 2012).

5.3.1.3 Blackholing Cooperative Defence

Blackholing strategy, which is also called as blackhole filtering, is used for dropping malicious network packets at the routing stage (Shameli-Sendi et al., 2015). This strategy achieves its aim by forwarding the harmful network packets to the Null0 virtual interface. While legitimate network traffic remains stable, each malicious network packet forwarded to the Null0 virtual interface is dropped immediately.

Blackholing cooperative defence strategy includes both DDoS attack detection techniques and routers (Shameli-Sendi et al., 2015). These detection techniques control the routers in order to blackhole the malicious network traffic which is generated together by different bots.

5.3.2 Non-collaborative-Static Strategy

This defence strategy is a non-collaborative mitigation approach, and it could not be reconfigured. Once a mitigation device is configured, mitigation techniques can only be applied when a DDoS attack is discovered by detection units (Shameli-Sendi et al., 2015).

A Confidence-Based Filtering strategy is proposed by Dou et al. (2013) for cloud computing. According to their model, the nominal characteristics of the systems are generated by analysing legitimate network packets during the non-attack period. Source IP address, total length, protocol type and time to live (TTL) attributes in the IP header, and destination port number and flag attributes in the TCP header are examined during the non-attack period in order to determine the nominal characteristics of the systems (Dou et al., 2013). The Nominal characteristics of the systems are used to discover DDoS attack traffic. With the help of the nominal characteristics of the systems, Confidence-Based Filtering strategy examines each network packet in order to understand whether it is an attack packet or not. If a network packet is considered malicious, it is discarded immediately.

5.3.3 Non-collaborative-Dynamic Strategy

5.3.3.1 Redirecting and Shunting

In this strategy, traffic is forwarded to another physical interface instead of being discarded. Then, a traffic analyser located on the alternate way can extract malicious traffic from real traffic and transmit the innocuous traffic to the servers. Currently, Software-Defined Networking (SDN) has been utilized to forward suspicious network traffic to these traffic analyser units (Shameli-Sendi et al., 2015).

Various DDoS protection mechanisms are based on this effective strategy (Shameli-Sendi et al., 2015). For instance, Cisco Guard and Riverhead Guard utilize from this strategy to mitigate massive DDoS attacks. The Cisco DDoS protection mechanism forwards malicious network packets to the Cisco Guard device. Then, this

device extracts harmful traffic from real network traffic and forwards the innocuous traffic to its destination (Shameli-Sendi et al., 2015).

5.3.3.2 Reconfiguration

This strategy makes changes to the defence method or topology of the target or the intermediary network systems to mitigate massive DDoS attacks (Shameli-Sendi et al., 2015). The reconfiguration strategy can be classified as service reconfiguration, defence reconfiguration and network reconfiguration according to the degree of reconfiguration.

- Service reconfiguration: This service-based reconfiguration strategy can be grouped as service regeneration and service cloning. Service regeneration aims to eliminate the security vulnerabilities of services and take back control of the compromised services. In this way, future DDoS attacks that will exploit the similar vulnerabilities can be prevented (Wang, 2005). However, in service cloning mitigation method, multiple instances of the same network service are installed at several points of the system and network traffic is distributed between these instances (Shameli-Sendi et al., 2015). Service cloning uses system resources efficiently to handle huge volumes of service requests; therefore, it is used widely in cloud computing to mitigate DDoS attacks (Yu et al., 2014).

- Defence reconfiguration: In this approach, the defence strategy can be reconfigured or its capability can be enhanced. In the first solution, the defence system is reconfigured to effectively deal with devastating DDoS attacks. In the second option, the defence mechanism is cloned to prevent DDoS attacks. Additionally, this cloning process can be triggered by service reconfiguration strategy to improve the capability of the defence mechanism (Yu et al., 2014). For instance, the DDoS defence mechanism can be automatically cloned if multiple instances of a network service are established in different parts of the system (Shameli-Sendi et al., 2015).

- Network reconfiguration: In order to mitigate or block massive DDoS attacks, this strategy reconfigures network topology by providing alternate paths. Service reconfiguration strategy uses shared or extra resources to stop DDoS attacks. However, this strategy changes network topology in order to prevent such attacks (Shameli-Sendi et al., 2015).

5.4 Summary

In this chapter, detailed information about DDoS attacks detection/mitigation strategies is provided. Firstly, anomaly-based and signature-based detection solutions are compared to reveal their strengths and drawbacks. Then, some of the most efficient mitigation mechanisms are examined to propose better mitigation strategies.

Signature-based solutions are efficient at detecting DDoS attacks if the signatures of them are created; therefore, these solutions could not detect new types of DDoS attacks before their signatures are created. However, new types of DDoS attacks can be detected by anomaly-based solutions if these new types generate exceptional system behaviour.

DDoS mitigation strategies both have benefits and drawbacks. These strategies can be integrated with detection solutions to provide more efficient DDoS protection strategies. Additionally, different DDoS mitigation strategies can be collaborated to increase the performance of the DDoS protection strategies.

Chapter 6

Conclusions and Recommendations

This dissertation has presented most important types of DDoS attacks and latest DDoS attack trends. Additionally, a comprehensive categorization of most widely used DDoS mitigation and detection strategies has been presented in order to demonstrate their limitations and strengths. Recently, DDoS attackers try to discover critical security vulnerabilities and utilize from attack mechanisms, such as botnets, DDoS amplification and IP spoofing, in order to launch more destructive DDoS attacks. Therefore, over the last few years, different types of DDoS attacks have emerged and the volume of DDoS attacks has extraordinarily increased.

Botnets have a crucial role in initiating destructive DDoS attacks. Attackers utilize from botnet handlers to control the bots of their botnets. However, harmful programs that are running on the bots of a botnet leave identifiable tracks and these tracks can be discovered by an advanced anti-virus software (Zargar et al., 2013). Thus, DDoS attackers have started to use alternative techniques, such as IRC and HTTP protocol, to provide communication with their botnets. Attackers also have the ability to control botnets using C&C channels, and they use botnets frequently to launch massive DDoS attacks. Furthermore, each bot of a botnet can be located in different places all over the world, and this distributed structure makes analysing botnet based DDoS attacks more challenging (Zargar et al., 2013). Hence, global botnet countermeasures and more efficient botnet detection mechanisms should be developed in order to deal with DDoS attacks that use botnets.

It is extremely challenging to deal with DDoS attacks and develop an efficient DDoS protection mechanism because each DDoS attack type has different structures and mitigation/detection techniques. Moreover, researchers could not easily implement and test their detection/mitigation solutions in a real environment or utilizing from real DDoS attack data. Additionally, DDoS detection and mitigation techniques have their limits, and DDoS attacks could not be prevented entirely. Thus, additional researches should be conducted on not only DDoS detection solutions but also DDoS mitigation solutions to provide stronger DDoS protection mechanisms (Shameli-Sendi et al., 2015).

Current DDoS protection solutions are sufficient in dealing with network layer and transport layer attacks; however, they are insufficient in dealing with application layer attacks. Thus, researchers and security experts have currently proposed new solutions for application layer attacks to mitigate and detect them. In application layer attacks, it is quite difficult to distinguish malicious attack traffic from normal network traffic because harmful traffic successfully completes each procedure which is required to be legitimate (Suryawanshi and Todmal, 2015). Additionally, in application layer attacks, attackers can carry out devastating DDoS attacks with establishing small numbers of UDP or TCP connections (Kumar, 2014). Moreover, application layer DDoS attacks are increasing extraordinarily because web applications have several weaknesses and current DDoS protection solutions are unaware of these vulnerabilities. Therefore, to cope with application layer attacks, software engineers should eliminate the security risks of their web applications in the software development lifecycle. Furthermore, custom security countermeasures should be developed and implemented to provide a complete defence strategy.

Anomaly-based and signature-based detection are the two most popular DDoS detection techniques. In signature based detection, DDoS attacks could not be discovered without knowing their signatures. Hence, new DDoS attack types could not be discovered by a signature-based detection technique before their signatures are created. However, in anomaly-based detection, new DDoS attack types could be discovered if they generate exceptional traffic patterns (Alomari et al., 2016).

DDoS mitigation mechanisms both have strengths and limitations. These mechanisms can be combined with DDoS detection mechanisms to enhance the ability of the defence strategy. Moreover, a DDoS mitigation mechanism can be triggered by other mitigation mechanisms to increase the efficiency of the defence strategy.

References

Alam, M. F. (2014). Application layer ddos a practical approach and mitigation techniques. [online] Retrieved from: https://conference.apnic.net/data/37/l7ddos_apricot_1393257782.pdf. [Accessed: 2016-01-09].

Alomari, E., Manickam, S., Gupta, B., Anbar, M., Saad, R. M., and Alsaleem, S. (2016). A survey of botnet-based ddos flooding attacks of application layer: Detection and mitigation approaches. In *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*, pages 52–79. IGI Global.

Arbor Networks (2012). The growing threat of application-layer ddos attacks. [online] Retrieved from: http://whitepapers.datacenterknowledge.com/content12127. [Accessed: 2016-01-09].

Arbor Networks (2016). Worldwide infrastructure security report. [online] Retrieved from: https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf. [Accessed: 2016-01-09].

Behal, S. and Kumar, K. (2016). Trends in validation of ddos research. *Procedia Computer Science*, 85:7–15.

Beitollahi, H. and Deconinck, G. (2012). Analyzing well-known countermeasures against distributed denial of service attacks. *Computer Communications*, 35(11):1312–1332.

Bhattacharyya, D. K. and Kalita, J. K. (2016). *DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance.* CRC Press.

CERT-UK (2014). Denial of service attacks: what you need to know. [online] Retrieved from: https://www.cert.gov.uk/wp-content/uploads/2015/01/Denial-of-service-attacks-what-you-need-to-know1.pdf. [Accessed: 2016-01-09].

Chen, L.-C., Longstaff, T. A., and Carley, K. M. (2004). Characterization of defense mechanisms against distributed denial of service attacks. *Computers & Security*, 23(8):665–678.

Chen, Y., Hwang, K., and Ku, W.-S. (2007). Collaborative detection of ddos attacks over multiple network domains. *IEEE Transactions on Parallel and Distributed Systems*, 18(12):1649–1662.

Cooke, E., Jahanian, F., and McPherson, D. (2005). The zombie roundup: Understanding, detecting, and disrupting botnets. *SRUTI*, 5:6–6.

Darwish, M., Ouda, A., and Capretz, L. F. (2013). Cloud-based ddos attacks and defenses. In *Information Society (i-Society), 2013 International Conference on*, pages 67–71. IEEE.

Dou, W., Chen, Q., and Chen, J. (2013). A confidence-based filtering method for ddos attack defense in cloud environment. *Future Generation Computer Systems*, 29(7):1838–1850.

Douligeris, C. and Mitrokotsa, A. (2004). Ddos attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, 44(5):643–666.

El-Soudani, M. M. and Eissa, M. A. (2003). Cooperative defense firewall protocol. In *Security and privacy in the age of uncertainty*, pages 373–384. Springer.

Feily, M., Shahrestani, A., and Ramadass, S. (2009). A survey of botnet and botnet detection. In *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, pages 268–273. IEEE.

Ferguson, P. and Senie, D. (2000). Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing (rfc-2827). Technical report.

Hashmi, M. J., Saxena, M., and Saini, R. (2012). Classification of ddos attacks and their defense techniques using intrusion prevention system. *International Journal of Computer Science & Communication Networks*, 2(5):607–614.

Hoque, N., Bhattacharyya, D. K., and Kalita, J. K. (2015). Botnet in ddos attacks: trends and challenges. *IEEE Communications Surveys & Tutorials*, 17(4):2242–2270.

Imperva (2016). Udp flood attacks. [online] Retrieved from: https://www.incapsula.com/ddos/attack-glossary/udp-flood.html. [Accessed: 2016-01-09].

Jun, J.-H., Lee, D., Ahn, C.-W., and Kim, S.-H. (2014). Ddos attack detection using flow entropy and packet sampling on huge networks. *ICN 2014*, page 196.

Karasaridis, A., Rexroad, B., Hoeflin, D. A., et al. (2007). Wide-scale botnet detection and characterization. *HotBots*, 7:7–7.

Karim, A., Salleh, R. B., Shiraz, M., Shah, S. A. A., Awan, I., and Anuar, N. B. (2014). Botnet detection techniques: review, future trends, and issues. *Journal of Zhejiang University SCIENCE C*, 15(11):943–983.

Kaspersky (2014). Global it security risks survey 2014 distributed denial of service (ddos) attacks. [online] Retrieved from: http://media.kaspersky.com/en/B2B-International-2014-Survey-DDoS-Summary-Report.pdf. [Accessed: 2016-01-09].

Kaspersky (2015). Global it security risks survey 2015: The current state of play. [online] Retrieved from: http://media.kaspersky.com/en/business-security/it-security-risks-survey-2015.pdf. [Accessed: 2016-01-09].

Kaspersky (2016). Kaspersky ddos intelligence report for q1 2016. [online] Retrieved from: https://securelist.com/analysis/quarterly-malware-reports/74550/kaspersky-ddos-intelligence-report-for-q1-2016/. [Accessed: 2016-01-09].

Kührer, M., Hupperich, T., Rossow, C., and Holz, T. (2014). Exit from hell? reducing the impact of amplification ddos attacks. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 111–125.

Kumar, G. (2014). Understanding denial of service (dos) attacks using osi reference model. *International Journal of Education and Science Research Review*, 1(5).

Mirkovic, J. and Reiher, P. (2005). D-ward: a source-end defense against flooding denial-of-service attacks. *IEEE transactions on Dependable and Secure Computing*, 2(3):216–232.

OWASP (2010). Application Layer (Layer 7) DDOS attacks. [online] Retrieved from: https://www.owasp.org/images/4/43/Layer_7_DDOS.pdf. [Accessed: 2016-01-09].

Owezarski, P. (2009). Implementation of adaptive traffic sampling and management, path performance.

Patcha, A. and Park, J.-M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer networks*, 51(12):3448–3470.

Pimentel, M. A., Clifton, D. A., Clifton, L., and Tarassenko, L. (2014). A review of novelty detection. *Signal Processing*, 99:215–249.

Shameli-Sendi, A., Pourzandi, M., Fekih-Ahmed, M., and Cheriet, M. (2015). Taxonomy of distributed denial of service mitigation approaches for cloud computing. *Journal of Network and Computer Applications*, 58:165–179.

Silva, S. S., Silva, R. M., Pinto, R. C., and Salles, R. M. (2013). Botnets: A survey. *Computer Networks*, 57(2):378–403.

Srivastava, A., Gupta, B., Tyagi, A., Sharma, A., and Mishra, A. (2011). A recent survey on ddos attacks and defense mechanisms. In *Advances in Parallel Distributed Computing*, pages 570–580. Springer.

Suryawanshi, N. A. and Todmal, S. (2015). Ddos attacks detection of application layer for web services using information based metrics. *International Journal of Computer Applications*, 117(9).

Tang, Y. and Chen, S. (2005). Defending against internet worms: A signature-based approach. In *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, volume 2, pages 1384–1394. IEEE.

Telelink (2013). Dos attack. [online] Retrieved from: http://itsecurity.telelink.com/dos-attack/. [Accessed: 2016-01-09].

Tyagi, A. K. and Aghila, G. (2011). A wide scale survey on botnet. *International Journal of Computer Applications*, 34(9):9–22.

US-CERT (2014). Ddos quick guide. [online] Retrieved from: https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf. [Accessed: 2016-01-09].

US-CERT (2015). The armada collective ddos amplification and mitigation recommendations. [online] Retrieved from: https://info.publicintelligence.net/US-CERT-ArmadaDDoS.pdf. [Accessed: 2016-01-09].

Vania, J., Meniya, A., and Jethva, H. (2013). A review on botnet and detection technique. *Int J Comput Trends Technol*, 4(1):23–29.

Wang, J. (2005). *Tolerating Denial-of-Service Attacks æ A System Approach*. PhD thesis, Citeseer.

Wang, P., Sparks, S., and Zou, C. C. (2010). An advanced hybrid peer-to-peer botnet. *IEEE Transactions on Dependable and Secure Computing*, 7(2):113.

Wong, F. and Tan, C. X. (2014). A survey of trends in massive ddos attacks and cloud-based mitigations. *International Journal of Network Security & Its Applications*, 6(3):57.

Yeshwantrao, S. A. and Jadhav, V. J. (2014). Threats of botnet to internet security and respective defense strategies. *International Journal of Emerging Technology and Advanced Engineering*, 4(1):121–127.

Yu, S., Tian, Y., Guo, S., and Wu, D. O. (2014). Can we beat ddos attacks in clouds? *IEEE Transactions on Parallel and Distributed Systems*, 25(9):2245–2254.

Yuce, E. (2011). A literature survey about recent botnet trends. ulakbim, turkey.

Zargar, S. T., Joshi, J., and Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. *IEEE Communications Surveys & Tutorials*, 15(4):2046–2069.