Doctoral Dissertation
博士論文

A Study on Observation of DRDoS Attacks for Proactive Countermeasure and Real-time Response

事前対策と即時対応を目的としたDRDoS攻撃の観測に関する研究

by

Daisuke MAKITA
牧田 大佑

Supervisor
Professor. Tsutomu MATSUMOTO

Graduate School of Environment and Information Sciences,
Yokohama National University
国立大学法人 横浜国立大学大学院 環境情報学府

March 2017

Acknowledgements

First, I would like to express my deepest appreciation to my supervisor Prof. Tsutomu Matsumoto for the tremendous support of my Ph.D. study and related research. His insights into my research and his valuable suggestions helped me in all the time. Besides him, I am incredibly grateful to Associate Prof. Katsunari Yoshioka, who taught me how to conduct research and write technical papers. Without his help, I would not have been able to finish my dissertation. I also gratefully acknowledge Prof. Junji Shikata, whose insightful comments and advice on the theoretical approaches have significantly contributed to improving my dissertation. I would like to thank Prof. Tatsunori Mori and Dr. Shin-ichi Shirakawa for serving on my dissertation committee. Their valuable comments and feedback were extremely helpful.

My sincere thanks also go to Mr. Koji Nakao, Dr. Daisuke Inoue, Dr. Junji Nakazato, Dr. Takahiro Kasama, Mr. Jumpei Shimamura, and all my colleagues at National Institute of Information and Communications Technology (NICT) for fruitful discussions, insightful comments, and the beneficial working environment. I also thank labmates and staff members in the Matsumoto Laboratory and the Yoshioka Laboratory at Yokohama National University: especially Mr. Hiroshi Mori, Dr. Yin Min Pa Pa, Mr. Rui Tanabe, Mr. Yoshiaki Nonogaki, Mr. Fumihiro Kanei, Mr. Shogo Suzuki, Mr. Takashi Koide, Mr. Takuya Tsutsumi, Ms. Tomomi Nishizoe, Ms. Mio Narimatsu, Ms. Tomoko Ishidate, Ms. Kumiko Nakayama, and Ms. Kiyono Yoshitani. The days we spent together are irreplaceable.

I would like to appreciate the following members we collaborated with in my research: Mr. Kosuke Murakami, Mr. Jumpei Urakawa, Ms. Yukiko Sawaya, Mr. Akira Yamada, and Mr. Ayumu Kubota at KDDI Research, Mr. Takemasa Kamatani and Mr. Wataru Senga at KDDI Corporation, Mr. Lukas Krämer, Mr. Johannes Krupp, and Dr. Christian Rossow at Saarland University in Germany, and Mr. Arman Noroozian, Dr. Maciej Korczyński, Dr. Carlos Hernandez Gañan, and Dr. Michel van Eeten at Delft University of Technology in Netherlands.

Last but not the least, I would like to thank my parents, sisters, relatives, and friends who support me throughout my life.

Abstract

Denial-of-Service (DoS) attacks have become a major threat on the Internet, and extensive researches have been made to tackle this threat. DoS attacks are often conducted by distributed hosts simultaneously to exhaust a resource of a target efficiently and to make it difficult to filter the attack traffic by administrators of the target. This type of DoS attack is called Distributed DoS (DDoS) attack. Since 2013, Distributed Reflection DoS (DRDoS) attacks, a.k.a amplification DDoS attacks, which abuse so-called *reflectors* to exhaust bandwidth of a target, have become one of the major methods to launch DDoS attacks, and there is a compelling need to take effective countermeasures. However, the details of DRDoS attacks are not well studied or reported, and therefore, it is necessary to observe DRDoS attacks and understand the trends and characteristics for effective countermeasures.

In this dissertation, we propose observation systems of DRDoS attacks, analyze DRDoS attacks that the systems observe, and propose countermeasures against DRDoS attacks using the systems.

First, we propose a system called DNS honeypot to observe DNS reflection attacks — a type of DRDoS attack that abuses *open resolvers* as reflectors. An open resolver is a DNS cache server that allows recursive queries from any clients on the Internet, and attackers abuse open resolvers as reflectors to launch DNS reflection attacks. DNS honeypot is a decoy open resolver which controls the traffic not to be involved in attacks, and it attempts to observe DNS reflection attacks from the reflector's point of view. We conducted a long-term experiment using two DNS honeypots and confirmed that the DNS honeypots were able to observe DNS reflection attacks and the number of attacks had increased since the middle of 2013. Besides, we analyze DNS reflection attacks that the DNS honeypots observed and reveal the trends and characteristics of the attacks, such as victims, abused domain names, and features included in packet headers.

Next, we analyze the correlation of DNS queries that the DNS honeypots and a darknet sensor observe. A darknet is unused IP address space (i.e. no legitimate hosts in its network), and most packets observed in a darknet stem from the results of malicious activities on the Internet, such as misconfigurations, backscatters of spoofed DDoS packets, and network probes. By comparing the DNS queries observed by DNS honeypots and a

darknet sensor, we attempt to reveal the relationship between DNS reflection attacks and scans of open resolvers. As a result of the analysis for half a year, we reveal that some attackers conduct scans of open resolvers using the same domain names as DNS reflection attacks before they launch attacks. This knowledge is expected to lead to proactive countermeasures such as the blacklisting of domain names used for DNS reflection attacks.

Not only DNS servers but also other open servers such as NTP and SSDP servers can be abused for DRDoS attacks. Therefore, we enhance DNS honeypot to DRDoS honeypot in order to observe not only DNS reflection attacks but also other types of DRDoS attacks from the reflector's point of view. We have gradually increased the number of honeypots and supported services, and we operate seven DRDoS honeypots with six services as of November 2015. To grasp the trends and characteristics of DRDoS attacks, we analyze 725,703 DRDoS attacks that the DRDoS honeypots observed for half a year from January to June in 2015. The result shows that 80% of the victims aggregated by the IP address suffered from a DRDoS attack only once for half a year and half of the attacks lasted only for less than five minutes. In addition, we find that 33% of the attacks went to only ten ASes and the victims are heavily biased.

Lastly, we propose DRDoS attack alert system using DRDoS honeypots as a countermeasure against DRDoS attacks. This alert system aims to help network administrators to grasp the situation of attacks quickly, and we expect that the administrators utilize this alert information for real-time responses such as mitigation and recovery. We have been operating this system and providing alerts of DRDoS attacks to several organizations under an R&D project in Japan. As a result of the operation, we compare detection times of attacks between the alert system and an ISP's mass traffic detector, and we confirm that the alert system can provide accurate and quick alerts for real-time responses.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

As the Internet has become core infrastructure in our daily lives, Denial-of-Service (DoS) attacks have become a major threat on the Internet. DoS attack is a kind of cyberattack that aims to make a system and/or a network unavailable and prevent legitimate users from accessing a specific resource of a target. Methods of DoS attacks are divided into two categories [1] [2]. One is that an attacker sends a malformed packet that exploits a vulnerability in a server program. If the server program has the vulnerability and has not fixed it yet, then the server program crashes and its service goes unavailable. The other one is that an attacker aims to consume a computational resource of a target (e.g. CPU and memory usage, network bandwidth, etc.). In particular, the latter type of DoS attack is often conducted by distributed hosts simultaneously to exhaust the resource efficiently and to make it difficult to filter the attack traffic by administrators of the target. This type of DoS attack is called Distributed DoS (DDoS) attack.

The incentives of DDoS attacks are various by attackers, but many of them can be divided into the following five categories: financial gain, revenge, ideological belief, intellectual challenge, and cyberwarfare [3]. For example, notorious hacker groups such as DD4BC [4] and Armada Collective [5] blackmail companies by DDoS attacks and demand ransom by Bitcoin[1]. Other groups such as Anonymous[2] conduct DDoS attacks for spreading their ideological belief.

Methods of DDoS attacks are also various, but many types of DDoS attacks are divided roughly into the following two categories: network-level DDoS and application-level DDoS [3]. The former methods mainly aim to flood

[1] A type of digital currency invented by Satoshi Nakamoto [6].

[2] An international hacker group which engages in protest activities under the name of "Anonymous." Some of the members conduct cyberattacks such as DDoS attacks to claim their belief.

network bandwidth of a target. For example, TCP SYN-Flood attacks, UDP-Flood attacks, and DNS reflection attacks are this type of attack. The latter methods aim to consume server resources such as CPU, memory, disk I/O, etc. For example, HTTP GET-Flood attacks and Slow Read DoS attacks are categorized into this type of attack.

This dissertation focuses on Distributed Reflection DoS (DRDoS) attacks — a kind of DDoS attack that floods communication bandwidth with amplified responses sent from open servers called *reflectors*. In DRDoS attacks, reflectors such as DNS servers and NTP servers that are available from anywhere on the Internet are abused by attackers, and a vast volume of traffic is generated from a relatively small volume of traffic. The method to launch DRDoS attacks was known around 2000 [7], and it has become one of the mainstream methods for DDoS attacks after the historic DDoS attack on Spamhaus[3] [8] in March 2013. According to Cloudflare [9], the attack was mainly conducted by DNS reflection attack, a type of DRDoS attack which abuses DNS servers as reflectors, and the volume of the traffic related to the attack reached 300 Gbps at the peak [10]. The analyst said that the DDoS attack almost broke the Internet. In addition, in February 2014, a DDoS attack against OVH[4] [11] was conducted and the volume of the traffic reportedly reached 400 Gbps from NTP servers [12]. Thus, the volume of traffic generated by DRDoS attacks is getting more and more terrible. As the impact of attacks is getting worse, hacker groups such as Anonymous and DD4BC utilize DRDoS attacks as a method to launch DDoS attacks. Furthermore, DDoS providing services called Booter or Stresser have emerged recently [13] [14] [15] [16], and ordinary users without the knowledge of DDoS attacks can easily launch DDoS attacks.

The threat of DRDoS attacks has been growing and there is a compelling need to take effective countermeasures. Many researchers have studied DRDoS attacks and published papers to work on this threat — such as approaches to preventing IP address spoofing [17] [18] [19] [20] [21] [22], reducing the impact of reflectors [23] [24] [25] [26] [27] [28], detecting and mitigating DRDoS attacks at a victim side [29] [30] [31] [32] [33] [34] [35] [36]. However, in spite of these tremendous efforts, the threat remains serious and the details of DRDoS attacks are not well studied or reported.

1.2 Contributions

This dissertation includes four main contributions to tackling the threat of DRDoS attacks.

[3] A non-profit organization that provides information on countermeasures against cyberattacks, especially focusing on spam-mail.

[4] A company that provides web hostings and cloud services in Europe.

1) Novel honeypots to observe DRDoS attacks (Chapter 3, 5)
First, we propose DNS honeypot to observe DNS reflection attacks in Chapter 3. Then, we enhance DNS honeypot to DRDoS honeypot in order to observe not only DNS reflection attacks but also other types of DRDoS attacks in Chapter 5. To the best of our knowledge, these honeypots are the first observation systems to observe DRDoS attacks. In general, we cannot observe DDoS attacks because attack traffic goes from attackers to victims directly. However, in the case of DRDoS attacks, we can observe attacks from the reflector's point of view by DRDoS honeypots because attackers abuse open servers on the Internet to launch DRDoS attacks.

2) Analysis of DRDoS attacks in the wild (Chapter 3, 5)
In these chapters, we also analyze DRDoS attacks that these honeypots observed on the Internet. The main findings of these analyses are as follows. In Chapter 3, we show the trends and characteristics of DNS reflection attacks such as victims, abused domain names, and features included in packet headers. In Chapter 5, we analyze 725,703 DRDoS attacks that the DRDoS honeypots observed from January to June in 2015. The result shows that 80% of the victims aggregated by the IP address suffered from a DRDoS attack only once for half a year and half of the attacks lasted only for less than five minutes. Besides, we find that 33% of the attacks went to only ten ASes and the victims heavily deviate. These results give us a new insight into DRDoS attacks that has not been comprehended well.

3) DNS reflection attacks vs. Scans (Chapter 4)
In Chapter 4, we analyze the correlation of DNS queries that DNS honeypots and a darknet sensor observe. A darknet is unused IP address space (i.e. no legitimate hosts in its network), and most packets observed in a darknet stem from misconfigurations, backscatters of spoofed DDoS packets, and network probes. As a result of the comparison of DNS queries between DNS honeypots and a darknet sensor, we discover that some attackers conduct scans of open resolvers using the same domain names as DNS reflection attacks before they launch attacks. This knowledge is expected to lead to proactive countermeasures against DNS reflection attacks such as the blacklisting of domain names abused for the attacks.

4) DRDoS attack alert system (Chapter 6)
As another countermeasure against DRDoS attacks, we propose DRDoS attack alert system utilizing DRDoS honeypots in Chapter 6. By monitoring and analyzing the traffic of DRDoS honeypots, the alert system provides alerts of DRDoS attacks to our collaborative organizations in real time. To the best of our knowledge, this is the first attempt that notifies the information of DRDoS attacks as alerts. We have been operating this system and providing

DRDoS attack alerts to several organizations under an R&D project in Japan. From the result of the operation, we confirm that the alert system can provide accurate and quick alerts to network administrators, and the system can be expected as a system to support real-time responses to DRDoS attacks.

1.3 Organization

The rest of this dissertation is organized as follows. Chapter 2 presents the background and related work of this study. Chapter 3 proposes DNS honeypot to observe DNS reflection attacks and analyzes DNS queries that the DNS honeypots observed. Chapter 4 analyzes the correlation of DNS queries between the DNS honeypots and a darknet sensor for proactive countermeasures. Chapter 5 extends DNS honeypot to DRDoS honeypot in order to observe not only DNS reflection attacks but also other types of DRDoS attacks, and analyzes the observation results of the DRDoS honeypots. Chapter 6 proposes DRDoS attack alert system using DRDoS honeypots for real-time responses. Lastly, Chapter 7 concludes this dissertation.

Chapter 2

Background and Related Work

Denial-of-Service (DoS) attack is a kind of cyberattack that attempts to make a system and/or a network unavailable and prevent legitimate users from accessing a specific resource of a target. DoS attacks are often conducted by distributed hosts simultaneously to exhaust the resource efficiently, and this type of DoS attack is called Distributed DoS (DDoS) attack. This dissertation focuses on Distributed Reflection DoS (DRDoS) attack, a type of DDoS attack that floods the communication bandwidth with amplified responses sent from open servers called *reflectors*.

To clarify the theme of this dissertation, this chapter presents the background and related work of DRDoS attacks. First, Section 2.1 explains the methodology of DDoS attacks. Next, Section 2.2 describes the methodology of DRDoS attacks and discusses the previous studies to look over existing countermeasures against DRDoS attacks.

2.1 DDoS Attack

DoS attack is a kind of cyberattack that aims to make a target offline, and methods of DoS attacks are divided into two categories [1] [2]: exploiting vulnerabilities and exhausting resources. The former methods are that an attacker sends a malformed packet that exploits a vulnerability in a server program. If the server program has the vulnerability and has not fixed it yet, then the server program crashes and its service goes unavailable. The latter methods are that an attacker aims to consume a computational resource of a target such as CPU, memory, and bandwidth of a network. In particular, the latter methods are often conducted by distributed hosts simultaneously to exhaust the resource efficiently and to make it difficult to filter the attack traffic by network administrators. This type of DoS attack is called Distributed DoS (DDoS) attack.

The incentives of attackers are also various and it is hard to comprehend their motivations. Zargar et al. summarize the incentives of DDoS attacks into five categories [3]: financial gain, revenge, ideological belief, intellectual challenge, and cyberwarfare. For example, hacker groups such as DD4BC [4] and Armada Collective [5] blackmail companies by DDoS attacks and demand ransom by Bitcoin. They are a typical type of attacker who aims financial gain. Other groups such as Anonymous conduct DDoS attacks for ideological belief (e.g. #OpKillingBay[1] [37]). Besides, an attacker conducted the historic DNS reflection attack against Spamhaus [8] for the revenge of the blacklisting by Spamhaus [10].

2.1.1 Methodology

The taxonomy of DDoS attacks is well studied and organized in the following literature [1] [2] [3] [38] [39] [40] [41]. The ways to categorize DDoS attacks are different in each literature, but most of the methods of DDoS attacks are divided roughly into the following two categories based on protocol level: network-level DDoS and application-level DDoS [3].

2.1.1.1 Network-level DDoS

Network-level DDoS attacks mainly aim to flood communication bandwidth of a victim by a vast volume of traffic. This type of DDoS attack focuses on exhausting resources of network/transport layers in Internet protocol suite, and attackers often spoof source IP addresses of packets to hide their identity and make it difficult to filter the attack packets.

Network-level DDoS attacks can be divided into the following four categories [3].

Flooding attacks

Attackers aim to exhaust network bandwidth of a victim by a large number of packets and disrupt connections from legitimate users. The remaining three types of network-level DDoS attacks are also categorized into this type of DDoS attack in a broad sense, but they have additional features for flooding.

e.g. UDP-Flood attack, ICMP-Flood attack.

Protocol exploitation flooding attacks

Attackers exploit specific features or implementation bugs to consume computational resources of a victim.

e.g. TCP SYN-Flood attack.

[1] An operation that targets websites of the Japanese government and companies participating in whale and dolphin hunting.

Reflection-based flooding attacks

Attackers aim to flood communication bandwidth of a victim by making open servers send responses to the victim by spoofing source IP addresses of requests. The open servers abused by attackers are called *reflectors*. This type of DDoS attack is called Distributed Reflection DoS (DRDoS) attack, and it is the main theme of this dissertation.

e.g. DNS reflection attack, NTP reflection attack.

Amplification-based flooding attacks

Attackers aim to consume network bandwidth of a victim by generating amplified responses with some specific services.

e.g. DNS amplification attack, NTP amplification attack.

Both reflection and amplification techniques are used at the same time so that attackers can flood the network bandwidth efficiently without being identified. Consequently, both reflection DDoS (i.e. DRDoS) and amplification DDoS often indicate the same type of network-level DDoS attack. In this dissertation, the term "DRDoS attack" means a type of DDoS attack that meets both reflection and amplification features.

2.1.1.2 Application-level DDoS

Application-level DDoS attacks mainly aim to consume machine resources such as CPU, memory, and disk I/O, etc. This type of DDoS attack consumes less network bandwidth than network-level DDoS attacks, and in most cases, attackers cannot spoof source IP addresses of packets because many protocols provide their services over Transmission Control Protocol (TCP) and TCP requires a three-way handshake before communication.

There are many protocols in application-layer, and therefore, in this section, we describe four methods of application-level DDoS attacks which exploit HTTP protocol [3].

Session flooding attacks

Attackers connect a web server and send an HTTP request repeatedly with the higher rate than legitimate users for exhausting resources of a server.

e.g. HTTP GET-Flood attack.

Request flooding attacks

Attackers send many HTTP requests to a web server in a single session.

e.g. HTTP GET-Flood attack.

Asymmetric attacks

Attackers send HTTP requests which require high costs to be processed.

Slow request/response attacks

Attackers send HTTP requests which require high costs to process and get/post data very slowly in order not to close the connection.

e.g. Slow Read DoS attack, HTTP fragmentation attack.

There are many types of application-level DDoS attacks, and these attacks have recently become severe threats on the Internet. Application-level DDoS attacks are beyond the scope of this dissertation and we do not give any more explanations about them, but we will address the problems of these threats in the future.

2.1.2 Launchers

To launch effective DDoS attacks, attackers need to have launchers of DDoS attacks. This section explains two types of launchers.

2.1.2.1 Botnet

A botnet is a network that consists of many computers infected with a bot program — a type of malicious software (malware) that executes commands from attackers. Botnets are often used to launch DDoS attacks for both network-level and application-level, and they have been involved in the major DDoS attacks on the Internet [42] [43].

Recently, botnets which consist of so-called "Internet of Things" (IoT) devices such as closed-circuit television (CCTV) cameras and digital video recorders (DVR) have become a severe threat on the Internet [44]. Some IoT devices provide a telnet service with a default pair of username and password, and therefore, they can be easily hacked by attackers. For example, one of the IoT botnets called "Mirai" consisted of approximately 380k infected devices and conducted a massive DDoS attack against "Krebs On Security"[2] [45] [46], and it is reported that the attack traffic was close to 620 Gbps [47].

2.1.2.2 Booter/Stresser

A booter, or stresser, is a service that provides DDoS attacks on the Internet [13] [14] [15] [16]. That is, if a customer pays money to a booter service and orders DDoS attacks, he/she can launch DDoS attacks without preparing launchers such as botnets. These services are provided under the name of a stress-test service of infrastructure, but they are often used to launch DDoS attacks by malicious customers (i.e. attackers).

Booter services provide many types of DDoS attacks (including both network-level and application-level DDoS. See Figure 2.1), and price for a subscription is relatively low (rather, some booter services provide free trials

[2] A popular blog site on cybersecurity by Brian Krebs.

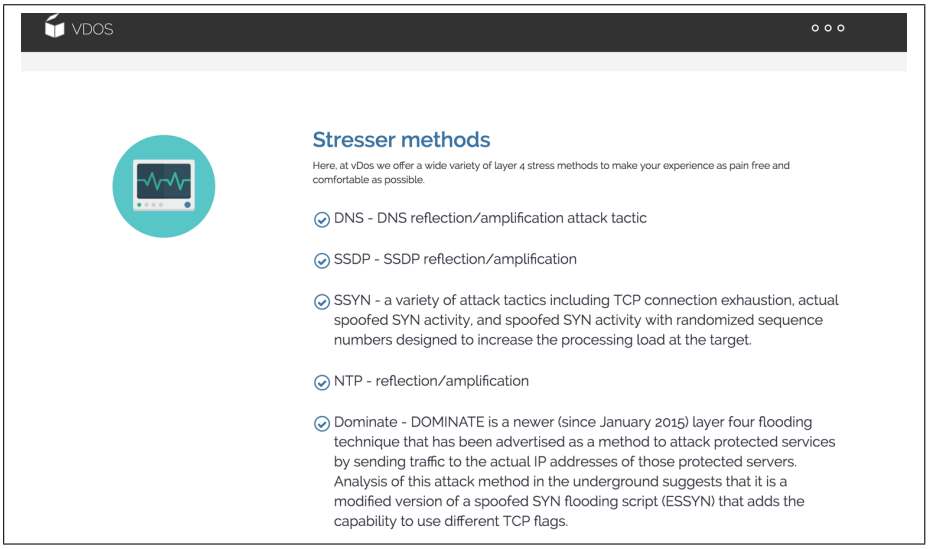


Figure 2.1: Screenshot of booter website (vDos).

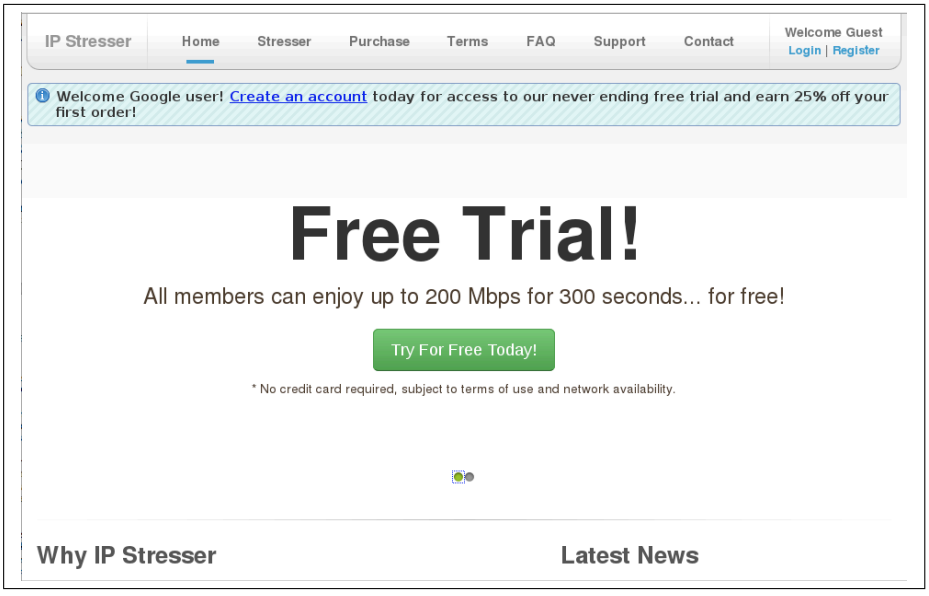


Figure 2.2: Screenshot of booter website (IP Stresser).

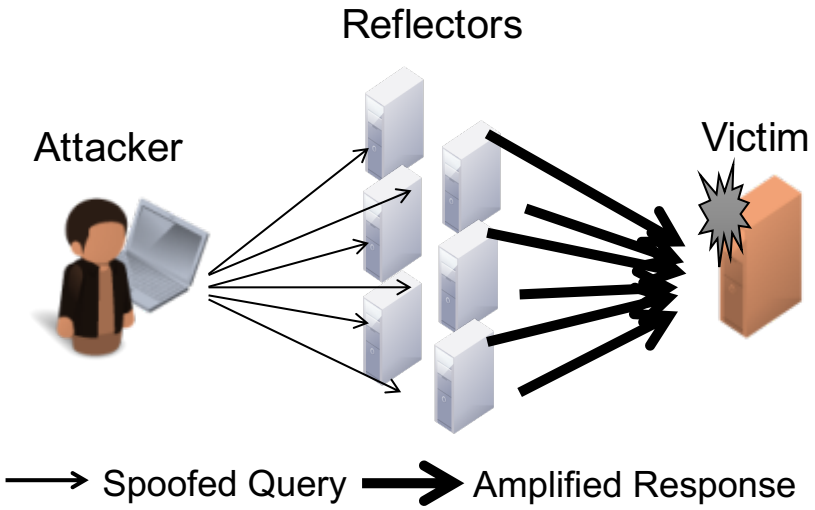


Figure 2.3: Scenario of DRDoS attack.

depending on attack conditions such as attack duration, the number of concurrent attacks, and the volume of attacks. See Figure 2.2). We can find these services by visiting underground forums or just querying related words such as "booter" and "stresser" on web engines. That is why booter services have become popular among malicious customers, and booter services have become the primary cause of recent DDoS attacks.

2.2 DRDoS Attack

This section provides the introduction of DRDoS attack techniques and existing countermeasures.

2.2.1 Methodology

DRDoS attack is a type of DDoS attack that floods communication bandwidth of a target by sending packets to the target via open servers. In this attack, services which meet the following features are abused by attackers.

Amplification
: In some protocols, the size of a response packet is larger than that of a request packet. Abusing this feature, attackers can generate a vast volume of traffic from a relatively small volume of traffic. From this feature, abused servers are called *amplifiers*.

Reflection
: Internet Protocol (IP) has no built-in mechanisms to verify a source IP

Table 2.1: Protocols that can be abused for DRDoS attacks [25].

Category	Protocol	Port(s)	Description
Legacy	QOTD	17	Quote of the day
	CHG	19	Character generator
Network	DNS	53	Domain name system
	NTP	123	Network time
	NetBios	137	NetBIOS name service
	SNMP	161	Network management
	SSDP	1900	Simple service discovery
P2P	BitTorrent	any	P2P filesharing
	Kademlia	any	P2P hashtable
Game	Steam	27015	Steam game engine
	Quake 3	27960	Quake3 game engine
Bots	ZeroAccess(v2)	164XY	P2P-based malware
	Sality	any	P2P-based malware
	Gameover	any	P2P-based banking trojan

address of a packet [48]. Therefore, some services which do not validate sources — such as protocols that provide their services over User Datagram Protocol (UDP) — send back response packets without checking the sources of the request packets. From this feature, abused servers are called *reflectors*.

Attackers conduct DRDoS attacks abusing these features (Figure 2.3). First, attackers send reflectors many request packets whose source IP addresses are spoofed to the IP address of a victim. The reflectors send response packets to the victim because they do not verify the source IP addresses of the requests. As a result, the amplified response packets concentrate at the victim, and the network bandwidth of the victim floods with them and the service goes offline.

2.2.2 Abused Services

Many services can be abused as protocols of reflectors by DRDoS attacks. Rossow revealed that 14 protocols such as DNS and NTP could be abused for DRDoS attacks considering the conditions of amplification factors and the number of reflectors on the Internet (Table 2.1) [25].

In addition to these protocols, researchers have found that TFTP (69/udp) [49] [50], RPC portmap (111/udp) [51], CLDAP (389/udp) [52], RIPv1 (520/udp) [53], MSSQL (1433/udp) [54] [55], Sentinel LM (5093/udp) [51], mDNS (5353/udp) [56], and 3-way handshake of TCP [57] can be exploited for DRDoS attacks.

2.2.3 Countermeasures

Many researchers and projects have tried to address the threat of DRDoS attacks, and Fabrice et al. studied and organized the results of the efforts well in survey literature [58].

This section explains the existing approaches for countermeasures against DRDoS attacks by the following criteria: prevention of source address spoofing, reduction of reflectors' impact, detection and mitigation.

2.2.3.1 Prevention of Source Address Spoofing

Source address spoofing is a core problem of the Internet architecture. Internet Protocol (IP) has no built-in mechanisms to verify a source IP address by default because the purpose of the protocol is to deliver packets to destination addresses [48]. IP address spoofing for malicious purposes was first discussed in 1989 [59], and the detailed analyses of the problem were carried out by Heberlein et al. [17]. In this section, we introduce recent activities in order to prevent source address spoofing.

Detecting Spoofable Network The MIT Spoofer Project [20] makes measurements of spoofable networks on the Internet. The project distributes a software package to test if a network is spoofable or not by sending several spoofed UDP packets to a server owned by the project. The results are published at the website [22], and it is said that approximately 25% of ASes in the world are currently vulnerable to IP spoofing as of November 2016 [22].

Kührer et al. examined whether ASes allow IP spoofing or not by utilizing the fact that some open resolvers that work as DNS proxies do not correctly change source IP addresses when forwarding DNS packets [24]. As a result, they found 2,063 ASes that allowed IP address spoofing.

These results show that many ASes on the Internet remains spoofable in spite of the efforts.

Ingress Filtering Filtering spoofed IP packets can be achieved by ingress filtering (a.k.a BCP 38) [18]. This technique uses the knowledge of the range of IP addresses allocated by the networks and drops spoofed incoming packets on the routers. The ingress filtering is effective for preventing spoofing, but not all network administrators adopt this because the filtering rules need to be maintained and updated, and if the rules become outdated or misconfigured, the filter may prevent legitimate traffic.

2.2.3.2 Reduction of Reflectors' Impact

The existence of reflectors is also the cause of DRDoS attacks. In this section, we introduce previous studies and current projects to decrease the impact of

reflectors on the Internet.

Lowering Amplification Factors As described in Section 2.2.1, "amplification" is a core feature of DRDoS attacks. For that reason, many researchers have made efforts to lower the amplification factors of services abused by DRDoS attacks.

One of the approaches to lowering the amplification factors is to disable vulnerable protocols for the amplification. Rossow revealed that at least 14 UDP protocols could be abused for DRDoS attacks and NTP had the highest amplification factor out of them [25]. The problem of the amplification in NTP comes from the "monlist" function, which is not utilized for time synchronization. Therefore, Kührer et al. attempted to lower the amplification factor of NTP servers by the campaign of disabling the function [24], and they succeeded in decreasing reflectors of NTP.

In the case of DNS, an "ANY" pseudo-type of DNS query raises the amplification factors. The "ANY" pseudo-type is used to retrieve all records registered in a domain, and attackers often abuse the record type for DNS reflection attacks. Therefore, administrators of DNS cache servers have begun disabling "ANY" requests of DNS queries. For example, CloudFlare [9], which provides CDN and DDoS protection service, has started disabling "ANY" requests in UDP packets [60].

Reducing Number of Reflectors In the case of the attack on Spamhaus, more than 30,000 open resolvers were abused [10]. To reduce the impact of reflectors, some organizations, such as Open Resolver Scanning Project [26], Open Resolver Project [27], The Measurement Factory [61], and Open NTP Project [28], play an active part in decreasing the number of reflectors. However, extensive cooperation is required to achieve this goal because not only misconfigured servers but also end users' devices such as home routers work as reflectors.

2.2.3.3 Detection and Mitigation

Research on the detection and mitigation of DRDoS attacks is also necessary for countermeasures. In this section, we describe defense techniques against DRDoS attacks at a victim side.

Kambourakis et al. propose a method to detect DNS reflection attacks using logs at a victim network [30] [31]. The method detects attacks by checking the pairs of outgoing DNS requests and incoming DNS responses, and they suggest a detector that works as a firewall to filter packets of DNS reflection attacks. Tsunoda et al. propose a more general algorithm to detect DRDoS attacks by matching the pair of a request and a response at the gateway of a victim [29], and extend their system [32]. Besides, Tao et al. propose a protection method using History-based IP Filtering (HIP) [62].

The HIP system attempts to filter packets which come from unseen addresses previously during periods of high congestion. Wei et al. suggest a detection method by analyzing the arrival rate of packets at a victim [33], and Dietzel et al. propose an approach to blackholing some specific addresses at the Internet Exchange Points [36].

Detection and mitigation techniques at a victim side described in this section take extra costs to detect attack packets. Therefore, these systems work well in some situation, but it might be ineffective for the current DRDoS attacks because the traffic of DRDoS attacks is so huge that the systems cannot handle.

Chapter 3

Observation of DNS Reflection Attacks using DNS Honeypots

3.1 Introduction

Domain Name System (DNS) plays an important role in mapping domain names to the information such as IP addresses on the Internet [63] [64]. DNS is also abused for malicious activities. In particular, open resolvers — DNS cache servers which allow recursive queries from anywhere on the Internet — are the main cause of DNS reflection attacks.

According to the Open Resolver Project [27], there are approximately 25 million open resolvers on the Internet, and these are abused for DNS reflection attacks. In the historic DDoS attack against Spamhaus [8] in March 2013, it is reported that the attacker used the DNS reflection attack as the main attack vector and the volume of the traffic related to the attack reached 300 Gbps [10]. In addition, the Prolexic Technologies [65] — a company that provides DDoS protection service — reported that it suffered from an attack of 167 Gbps at the end of May 2013. Thus, in recent years, damages caused by DNS reflection attacks have become severe, and there is a compelling need for effective countermeasures. However, the details of these attacks are not well studied or reported, and it is necessary to observe DNS reflection attacks and understand their trends and characteristics.

In this chapter, we propose DNS honeypot to observe malicious activities which abuse DNS servers on the Internet. DNS honeypot is a decoy DNS cache server and attempts to observe DNS reflection attacks from the reflector's point of view. As a result of long-term experiments over one year, we confirm that DNS honeypot is useful for observing and analyzing DNS reflection attacks. In addition, we analyze the trends and characteristics of DNS reflection attacks that our two DNS honeypots observed, such as victims, abused domain names,

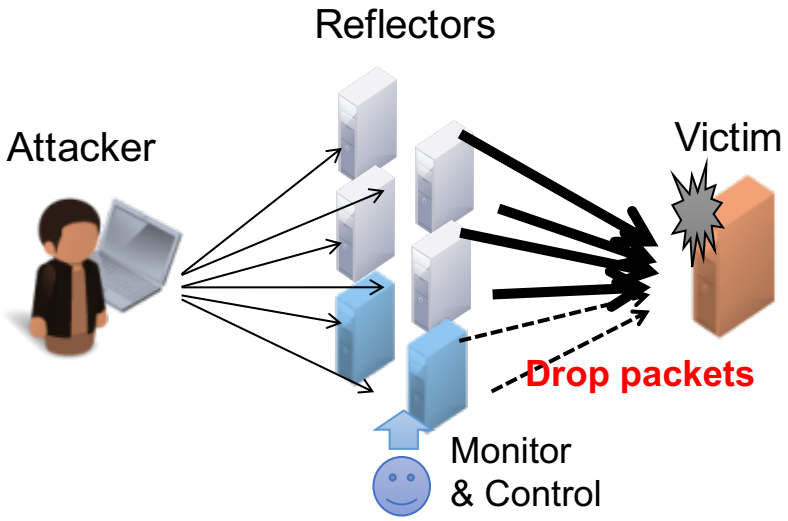


Figure 3.1: Idea of DNS honeypot.

and features included in packet headers.

The rest of this chapter is organized as follows. Section 3.2 explains the architecture and implementation of DNS honeypot. Section 3.3 describes the experiments and evaluations of the DNS honeypot, and Section 3.4 gives the case studies of DNS reflection attacks that the DNS honeypots observed. Section 3.5 discusses the results, and Section 3.6 summarizes this chapter.

3.2 DNS Honeypot

In this section, we explain the architecture and implementation of DNS honeypot. A honeypot is a computational resource used for observation and analysis of malicious activities. DNS honeypot is a decoy DNS cache server that works as an open resolver. In the case of DNS reflection attacks, we operate DNS honeypots on the Internet and observe DNS reflection attacks from the open resolvers' point of view (Figure 3.1).

3.2.1 Requirements

We set two requirements to be satisfied for DNS honeypot: "Observability" and "Safety."

Observability

"Observability" means that DNS honeypot is able to observe malicious activities by attackers on the Internet. In this study, we attempt to observe DNS reflection attacks. To satisfy this requirement, DNS honeypot needs to behave as an open resolver.

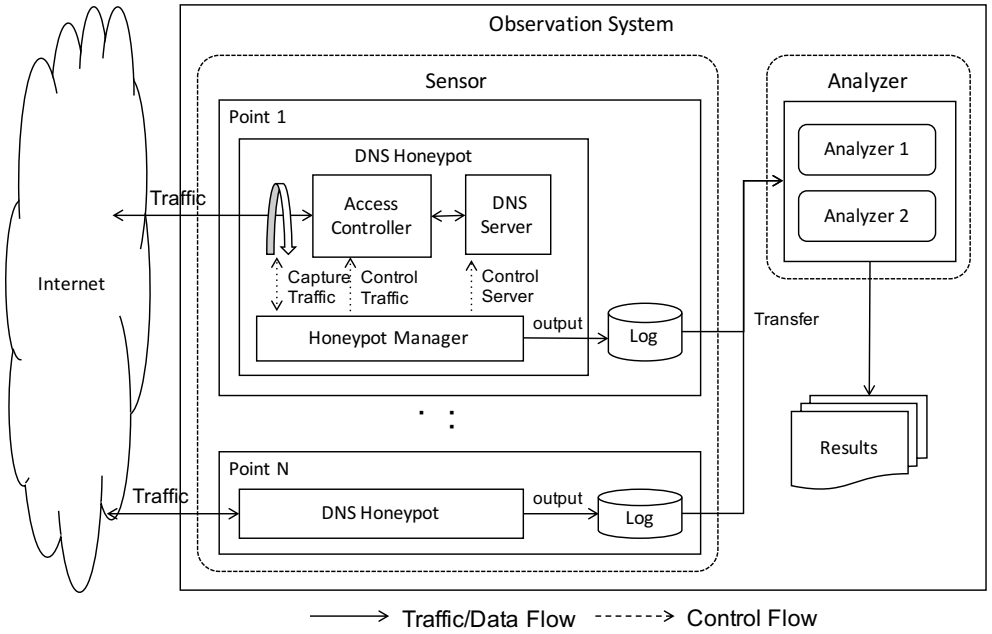


Figure 3.2: Architecture of DNS honeypot and observation system.

Safety

"Safety" means that DNS honeypot is able to observe malicious activities without affecting external environments such as victims and Internet Service Providers (ISPs). To satisfy this requirement, DNS honeypot needs to control traffic in order not to be involved in attacks.

Considering the nature of DNS reflection attacks, if we do not restrict outgoing packets, then DNS honeypots help attackers to conduct the attacks. On the other hand, if we heavily restrict outgoing packets, then DNS honeypots might not be able to observe DNS reflection attacks because some attackers might test the ability of reflectors. Therefore, "Observability" and "Safety" are in a trade-off relationship, and it is necessary to adjust these requirements for the purpose.

3.2.2 Architecture

Figure 3.2 shows the architecture of DNS honeypot and the observation system. DNS honeypot aims to observe and analyze DNS reflection attacks that abuse open resolvers, and it consists of three components: "DNS Server," "Access Controller," and "Honeypot Manager."

DNS Server

"DNS Server" plays a role to work as an open resolver.

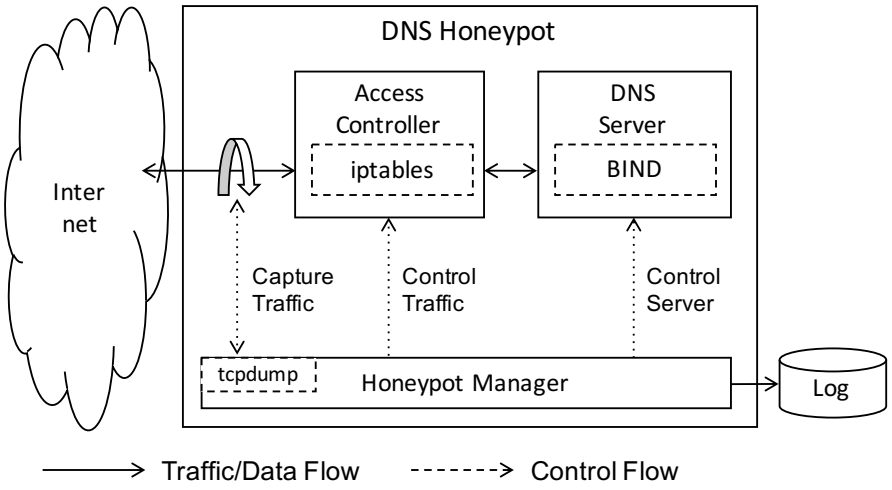


Figure 3.3: Implementation of DNS honeypot.

Access Controller

"Access Controller" is located in between the Internet and the "DNS server," and controls traffic of the "DNS server" when it is abused by attackers.

Honeypot Manager

"Honeypot Manager" controls "DNS Server" and "Access Controller," and outputs logs of DNS honeypot.

In general, when analyzing the traffic of honeypots, it is better to analyze data of multiple honeypots for comparison and correlation. Therefore, we divide the observation system into two parts as shown in Figure 3.2: "Sensor" and "Analyzer."

Sensor

"Sensor" includes several observation points connected to the Internet. In each observation point, DNS honeypot works as an open resolver and collects data of DNS packets.

Analyzer

The data collected by the "Sensor" are transferred to "Analyzer," where the data are analyzed and output results are generated.

3.2.3 Implementation

We implement DNS honeypot as shown in Figure 3.3. At each observation point, we prepare a machine which installs Ubuntu [66], one of the most popular Linux distributions. On the Ubuntu machine, BIND [67] works as

Table 3.1: Observation environments of DNS honeypots.

	DNS-HONEY1	DNS-HONEY2
Location	Japan	
ISP	ISP-A	ISP-B
Function	Open Resolver	
Observation period	Oct. 7th, 2012 to Oct. 31st, 2013	May 20th, 2013 Oct. 31st, 2013
Days	390 days	165 days
Change of IP addrs.	9 times	5 times

"DNS Server," iptables [68] works as "Access Controller," and standard Linux commands and original shell scripts work as "Honeypot Manager." The traffic of DNS honeypot is captured by tcpdump [69] as a libpcap file format [70], and pcap files are generated as output logs.

3.3 Experiments and Results

In this section, we describe the experiments and results of DNS honeypots. The purpose of the experiments is to verify whether DNS honeypot is able to observe DNS reflection attacks, and analyze the trends and characteristics of the attacks.

In this chapter, we analyze DNS queries that our DNS honeypots observed focusing on the following points: the number of DNS queries, geolocation of the source IP addresses (i.e. victims), and Fully Qualified Domain Names (FQDNs) used for DNS reflection attacks. In addition, we analyze field values included in packet headers of DNS queries and reveal the features included in the packets of DNS reflection attacks.

3.3.1 Experiments

In the experiments, we firstly verified whether attackers abused DNS honeypot or not by using an instance of DNS honeypot under an ISP network in Japan (DNS-HONEY1). After confirming that DNS honeypot was able to observe DNS reflection attacks, we added another DNS honeypot under another ISP network (DNS-HONEY2). In this chapter, we analyze traffic that the two DNS honeypots observed.

Table 3.1 shows the overview of the environments of each observation point. Two observation points belong to each ISP network in Japan, and DNS honeypots work as an open resolver.

At the beginning of the observation, we did not restrict outgoing traffic to give priority to "Observability", but we started filtering outgoing packets up to 1 pps (packets per second) using a hashlimit module of iptables in order not to

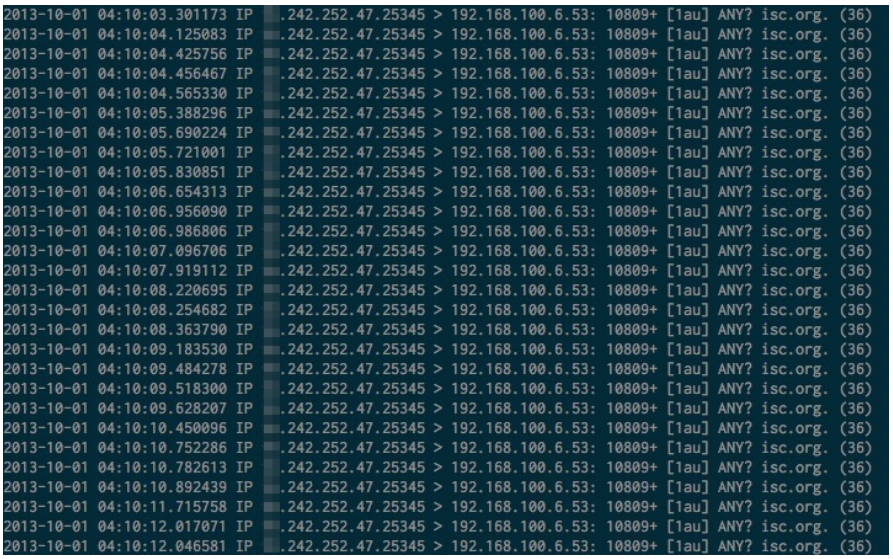


Figure 3.4: Example of packets observed by DNS honeypot.

be involved in attacks (for "Safety") after August 3rd, 2013 at DNS-HONEY-1 and May 27th, 2013 at DNS-HONEY2 respectively. Note that DNS-HONEY1 changed its global IP addresses nine times and DNS-HONEY2 changed its global IP addresses five times during the observation periods.

3.3.2 Results

Since DNS honeypots are not a public service, traffic that the DNS honeypots observe is highly related to malicious activities such as scans and DNS reflection attacks. However, the traffic we estimate as DNS reflection attacks has a variety of execution methods (e.g. traffic volume, the number of target IP addresses, attack duration, etc.), and therefore, it is difficult to determine the definition of DNS reflection attacks.

In this chapter, we analyze DNS reflection attacks based on the number of DNS queries that the DNS honeypots observed. The number of DNS queries of DNS reflection attacks is much larger than that of scans (Figure 3.4), and therefore, the statistics of the DNS queries strongly reflect the trends and characteristics of the DNS reflection attacks.

We give case studies of DNS reflection attacks in Section 3.4, and later in this section, we analyze the observation results focusing on the following three points: the number of DNS queries, geolocation of the victims, and abused FQDNs.

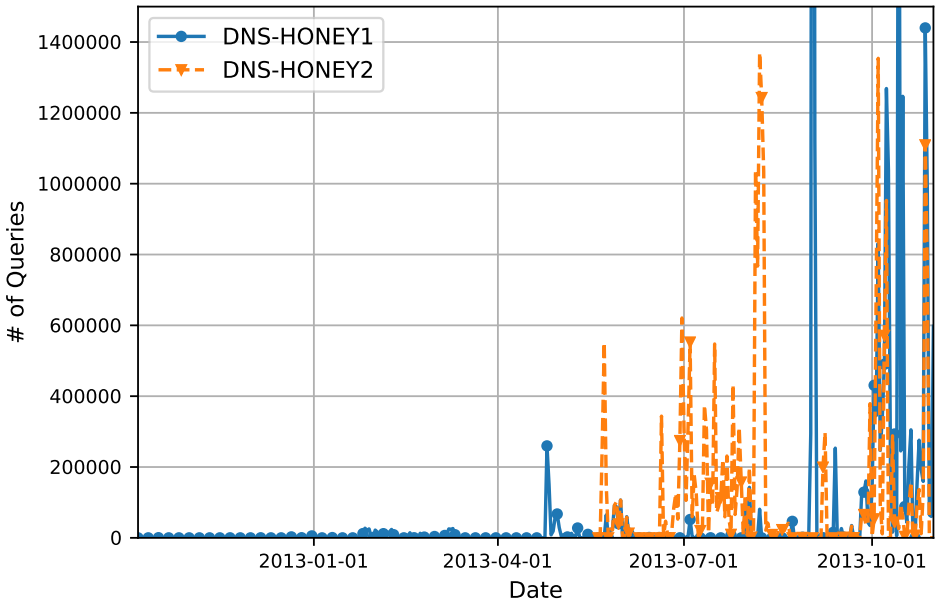


Figure 3.5: Number of DNS queries observed by DNS honeypots.

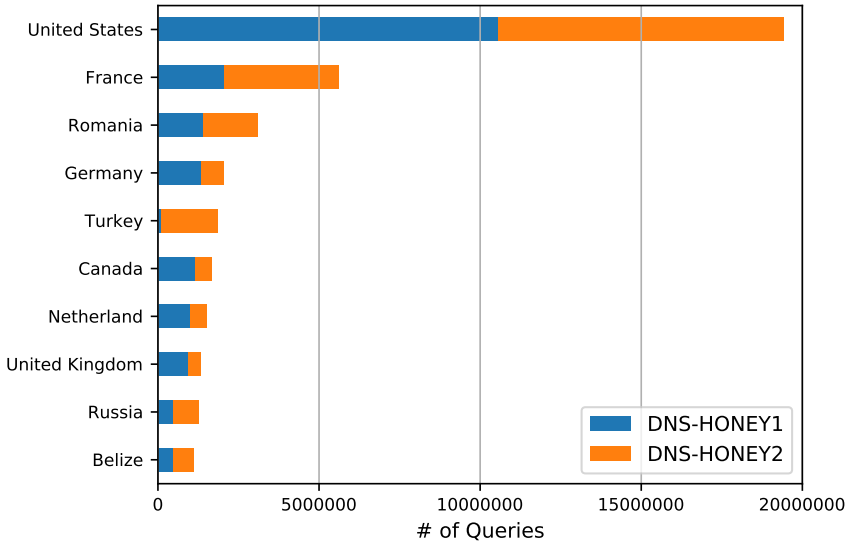
Table 3.2: Observation results of DNS honeypots.

	DNS-HONEY1	DNS-HONEY2
# of DNS queries	24,600,390	22,169,789
# of source IP addresses	16,546	8,145
# of FQDNs	1,363	174

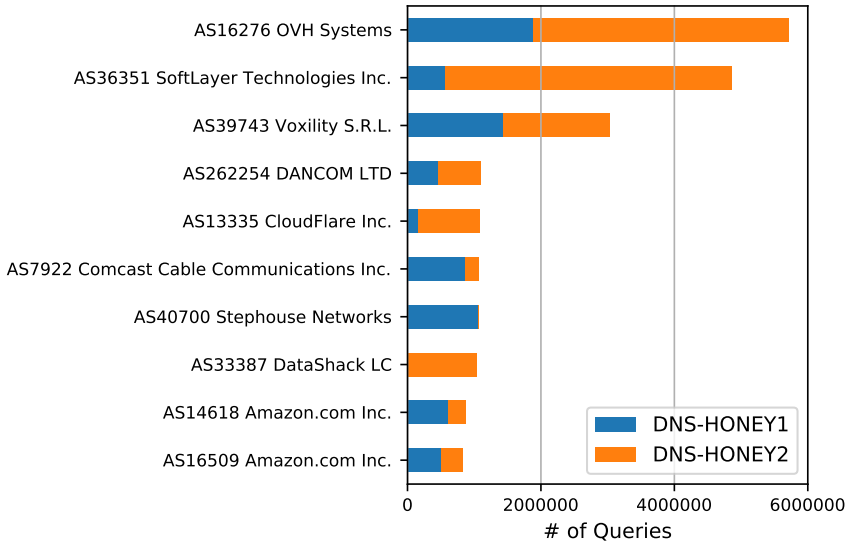
3.3.2.1 Number of DNS Queries

Figure 3.5 shows the number of DNS queries observed by the DNS honeypots. As a whole of the trend, the DNS honeypot did not observe DNS reflection attacks at the beginning of observation in October 2012, but the number of queries had increased since the second half of April 2013. In particular, on September 2, 2013, DNS-HONEY1 had observed more than five million DNS queries in a day, and hundreds of thousands of DNS queries were observed per day since October 2013.

Table 3.2 shows an overview of DNS queries that the two DNS honeypots observed during the observation periods. The DNS honeypots observed nearly 47 million DNS queries in total. As a result of the analysis, 99.9% or more of DNS queries requested recursive queries, and 99.5% or more of queries requested EDNS0 (Extension Mechanisms for DNS) [71]. EDNS0 is an extension for transferring data larger than 512 octets in UDP packets. These results show that most of the DNS queries tried to get large responses



(a) Countries (TOP 10).



(b) ASes (TOP 10).

Figure 3.6: Geolocation of source IP addresses observed by DNS honeypots.

for amplification.

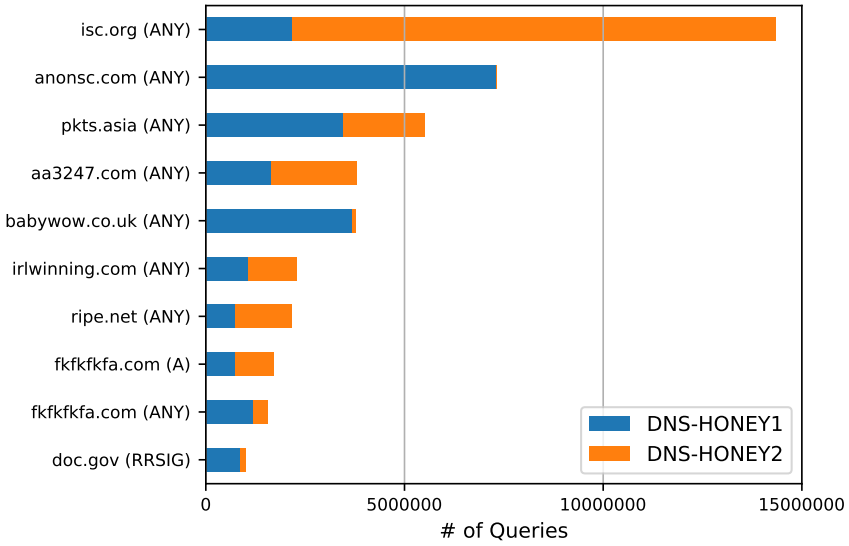


Figure 3.7: FQDNs observed by DNS honeypots (TOP 10).

3.3.2.2 Countries and ASes

We looked up countries and Autonomous Systems (ASes) of source IP addresses (i.e. victims of DNS reflection attacks) using GeoIP Lite databases by MaxMind [72]. Figure 3.6a and 3.6b show the geolocation of the victims of DNS reflection attacks observed by the DNS honeypots. Looking at countries, the United States was the most targeted, followed by Western countries such as France and Romania. Looking at ASes, OVH Systems, which provides hosting services in Europe, was the most targeted, followed by companies which provide web hostings and cloud services.

3.3.2.3 FQDNs Used for DNS Reflection Attacks

Figure 3.7 shows TOP-10 FQDNs of DNS queries observed by the DNS honeypots. The honeypots observed many requests of the "ANY" pseudo record. To send a DNS query, a pair of a domain name and a resource record type (e.g. "A" record points an IP address, and "NS" record points a hostname of an authoritative nameserver) is required. By specifying the "ANY" pseudo record of a domain name, we can obtain all records registered in the domain name, and this record type leads to a large response with a high amplification factor.

Table 3.3 shows the response sizes and amplification factors of popular FQDNs and FQDNs observed by the DNS honeypots respectively. Here, we analyze TOP-10 FQDNs which Alexa Internet [73] published on its website as popular FQDNs. Compared to the popular FQDNs, the FQDNs observed by

Table 3.3: Response sizes and amplification factors of FQDNs.

(a) Popular FQDNs.

FQDN	Type	Response size [Byte] [a]	Amplification factor [%] [b]
google.com	ANY	644	847 %
facebook.com	ANY	258	361 %
youtube.com	ANY	611	796 %
yahoo.com	ANY	446	610 %
baidu.com	ANY	476	648 %
wikipedia.org	ANY	366	486 %
qq.com	ANY	85	165 %
live.com	ANY	604	818 %
linkedin.com	ANY	927	1167 %
twitter.com	ANY	780	1002 %

(b) FQDNs observed by DNS honeypots.

FQDN	Type	Response size [Byte] [c]	Amplification factor [%] [b]
isc.org	ANY	3542	4541 %
anonsc.com	ANY	- [d]	- [d]
pkts.asia	ANY	4056	5070 %
aa3247.com	ANY	4357	5379 %
babywow.co.uk	ANY	4610	5488 %
irlwinning.com	ANY	4061	4778 %
ripe.net	ANY	3266	4134 %
fkfkfkfa.com	A	3993	4811 %
fkfkfkfa.com	ANY	4067	4900 %
doc.gov	RRSIG	11390	14603 %

[a] As of November 25th, 2013.

[b] Amplification factor (AF) is calculated by the following formula.

$$AF = \frac{Sizeof ResponsePacket}{Sizeof RequestPacket} \times 100[\%] \quad (3.1)$$

The size of a packet is the sum of Ethernet header size (14 bytes), IP header size (20 bytes), UDP header size (8 bytes) and payload size.

[c] Maximum response size during the observation period.

[d] Undefined because we could not estimate the response size.

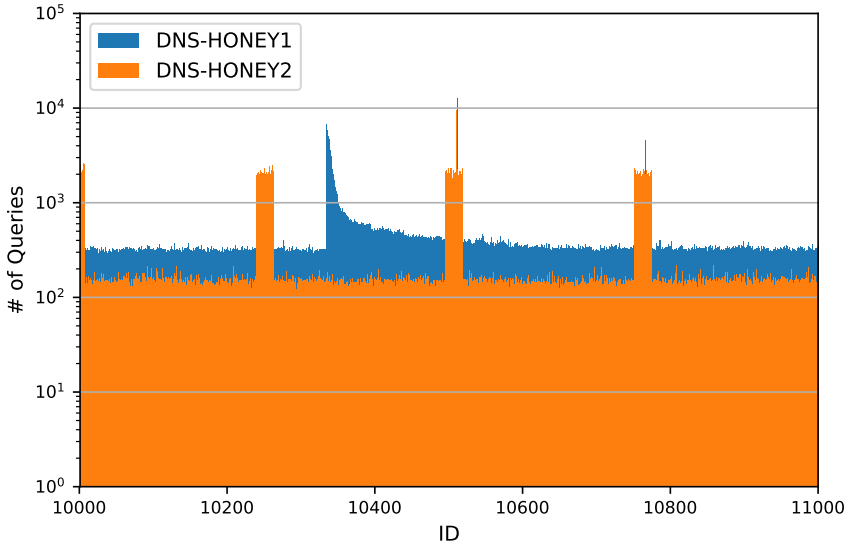


Figure 3.8: Distribution of ID values in IP header (from 10000 to 11000).

DNS honeypots have large responses and their amplification factors are high enough to be easily exploited for DNS reflection attacks.

3.3.3 Analysis of Packet Headers

In this section, we analyze DNS queries focusing on field values in IP, UDP and DNS headers. As a result of the analysis, we confirm that significant features exist in ID and Time-To-Live (TTL) values in IP header, source port numbers in UDP header, and ID values in DNS header. We explain the overview of these fields and the features we found.

3.3.3.1 ID Values in IP Header

The ID field value in IP header is a 16-bit identifier used for fragmentation and reconstruction of IP packets. The allocation of ID values depends on the system implementation, but on the nature of the identifier, it is required not to overlap values [74].

Figure 3.8 shows the distribution of ID values in IP header. Most of the ID values are distributed uniformly, but some of the ID values were frequently observed. In particular, DNS-HONEY2 observed high frequencies of ID values with 256 intervals. We investigated and found that some DNS reflection attacks used a single or some range of ID values in an attack.

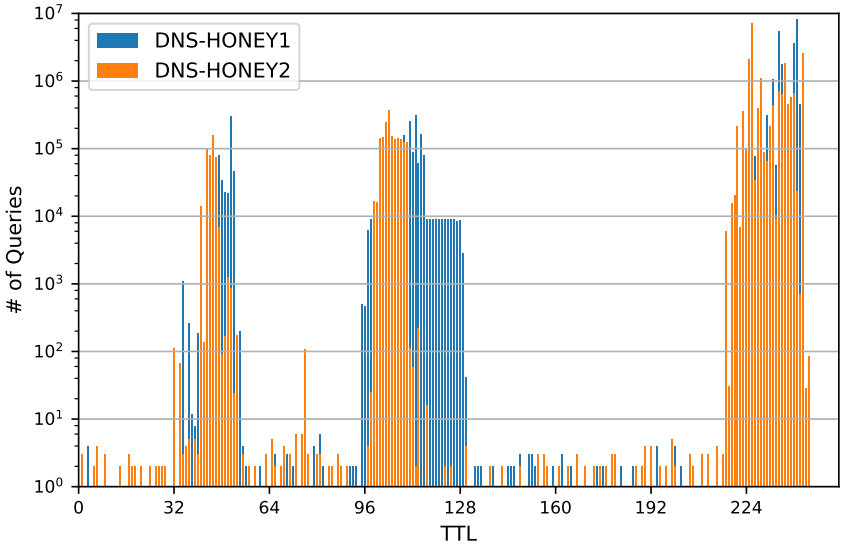


Figure 3.9: Distribution of TTL values in IP header.

3.3.3.2 TTL Values in IP Header

The TTL field value in IP header is an 8-bit integer value that represents the lifetime of the IP packet. In the current implementation, the value decreases one by one every time the packet hops a router, and when the value reaches zero, the packet is dropped by the router. That is how the Internet prevents the infinite loop of packets.

The initial value of TTL is characteristic for each operating system. In the case of a UDP packet, Windows OS after Windows XP uses 128, MacOS X and Ubuntu 12.04 use 64 respectively. On the Internet, the number of hops to reach a destination host is said to be up to 30. Therefore, most implementations adopt values which are more than 30 hops and a power of 2 (i.e. 32, 64, 128, 255).

Figure 3.9 shows the distribution of TTL values in IP header. From this figure, most of the TTL values of DNS queries observed by the DNS honeypots were classified into three initial values: 64, 128, 255.

3.3.3.3 Source Port Numbers in UDP Header

The source port number in UDP header is a 16-bit integer value used for communication between computers. DNS servers listen on port 53 by default, but a port number that client programs use is system-dependent. However, in recent systems, it is required to select random ports in order to prevent DNS cache poisoning attack [75] [76]. Therefore, the distribution of source port numbers should be uniform except for the range of well-known port numbers

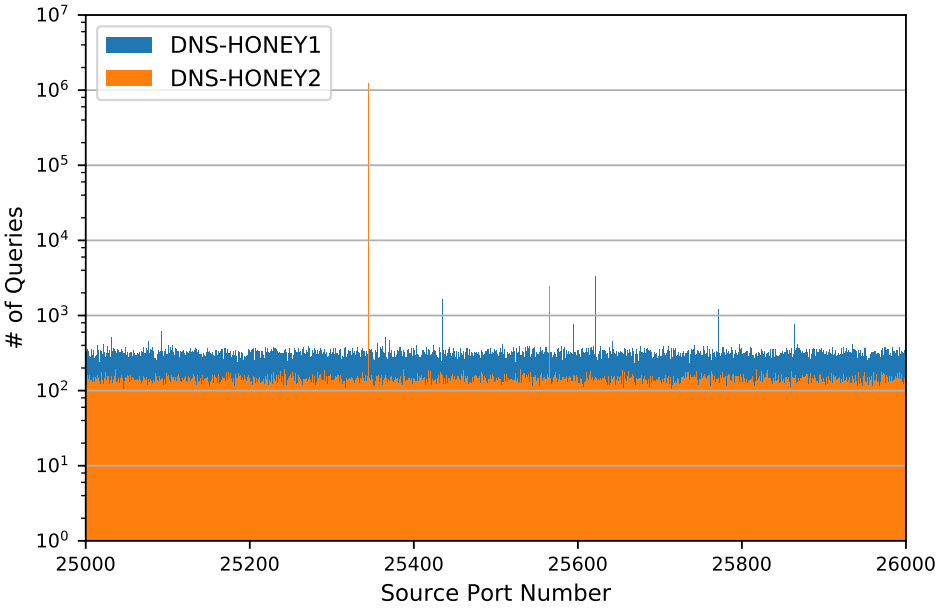


Figure 3.10: Distribution of source port numbers in UDP header (from 25000 to 26000).

that are not used for client programs in TCP/IP network.

Figure 3.10 shows the distribution of source port numbers of DNS queries observed by the DNS honeypots. From this figure, the number of DNS queries has been averagely distributed in the most port numbers, but we found that some port numbers were frequently used. We investigated and confirmed that some DNS reflection attacks used specific source port numbers, and we believe that this is because some attack tools use the same ports for sending queries effectively. In addition, we found that some attacks used well-known ports as source port numbers, such as 22 (SSH) and 80 (HTTP). We believe that this is because packets which uses well-known ports may not be filtered by firewalls if victims provide services on the ports.

3.3.3.4 ID Values in DNS Header

The ID field value in DNS header is a 16-bit integer for identifying the correspondence between a request and a response of DNS communication. Assignment of ID values is system-dependent, but on the nature of the identifier, each value should be different by the query. In addition, because of the threat of DNS cache poisoning attack, the value also needs to be randomly selected [75] [76]. Therefore, the distribution of ID values in DNS header should be uniform.

Figure 3.11 shows the distribution of ID values in DNS header of DNS

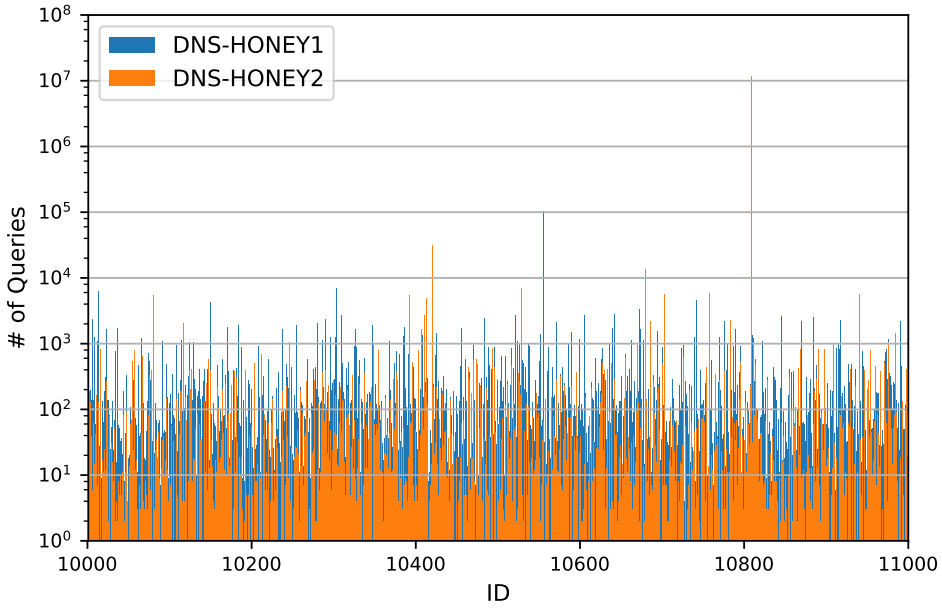


Figure 3.11: Distribution of ID values in DNS header (from 10000 to 11000).

queries observed by the DNS honeypots. The distribution of ID values in DNS header are not uniform compared to ID values in IP header or source port numbers in UDP header, and we confirmed that some of the ID values were frequently used in DNS reflection attacks.

3.4 Case Studies

In this section, we describe two examples of DNS reflection attacks that our DNS honeypots observed during the observation period.

3.4.1 Case I: Attack against DDoS Protection Provider

Our DNS honeypots observe many DNS reflection attacks against DDoS protection providers. In this section, we explain an attack against a famous DDoS protection service in May 2013.

This attack was observed by DNS-HONEY2 from 05:34 a.m. on May 22nd, 2013 (JST[1]). The target consisted of five IP addresses owned by the provider, and the pairs of FQDNs and record types of DNS queries were www.58wgw.com (ANY) and ripe.net (ANY).

Figure 3.12 shows the number of DNS queries that DNS-HONEY2 observed during this attack. This attack lasted for one and half a day with some breaks.

[1]Japan Standard Time

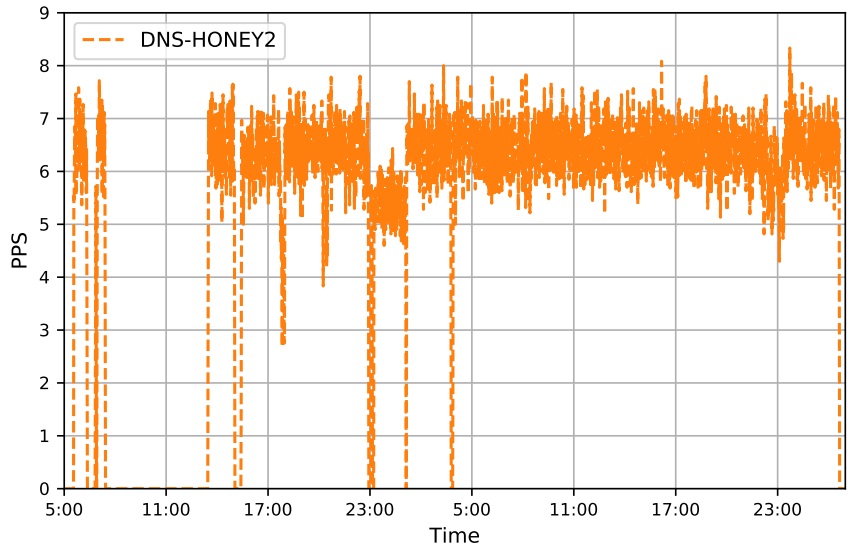


Figure 3.12: Case I: Number of DNS queries.

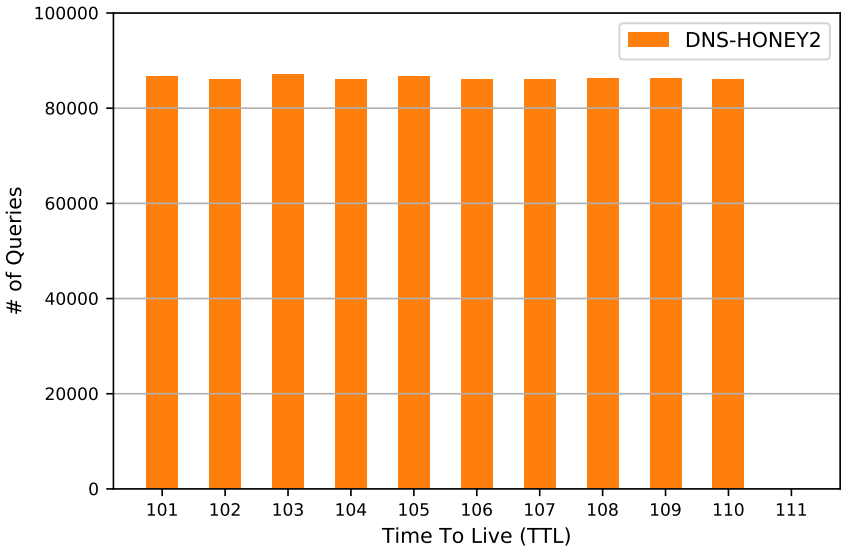


Figure 3.13: Case I: Distribution of TTL values.

The TTL values of DNS queries are distributed from 101 to 110 (Figure 3.13). This means that there were more than ten routes from the actual packet sender(s) to the DNS honeypot, and this result shows that there were more than ten hosts which sent DNS queries to the honeypot. Furthermore, we confirmed a large deviation in the distribution of the ID values in DNS header

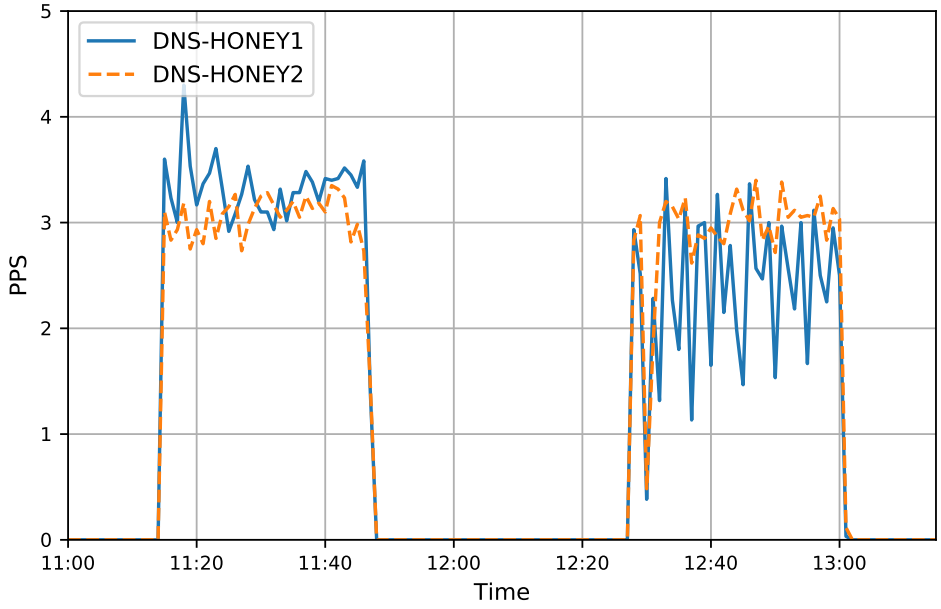


Figure 3.14: Case II: Number of DNS queries.

in this attack. From these results, we suppose that these packets were made by a specific packet generation program. This indicates that the attacker launched this attack by his/her botnet.

3.4.2 Case II: Attack against /24 Network

Many of DNS reflection attacks target only a single IP address at the same time. However, we observed an attack against one hundred of IP addresses in the same /24 network on May 29th, 2013.

This attack was observed from 11:14 a.m. on May 29th, 2013 (JST) by both DNS-HONEY1 and DNS-HONEY2. The pair of an FQDN and its record type was ripe.net (ANY). The target IP addresses were in the same /24 network, and the fourth octet values were distributed from 1 to 100.

Figure 3.14 shows the number of DNS queries that our DNS honeypots observed. Both start and end times of the attack are the same between the two honeypots. In addition, TTL values are averagely distributed from 107 to 116 in DNS-HONEY1 and from 101 to 110 in DNS-HONEY2 respectively.

Figure 3.15 shows the changes of target IP addresses in time series. The X-axis represents the time, and the Y-axis indicates the target IP addresses. From this figure, the target IP addresses changed mechanically based on the time, and this result shows that the attacker intentionally distributed the target IP addresses.

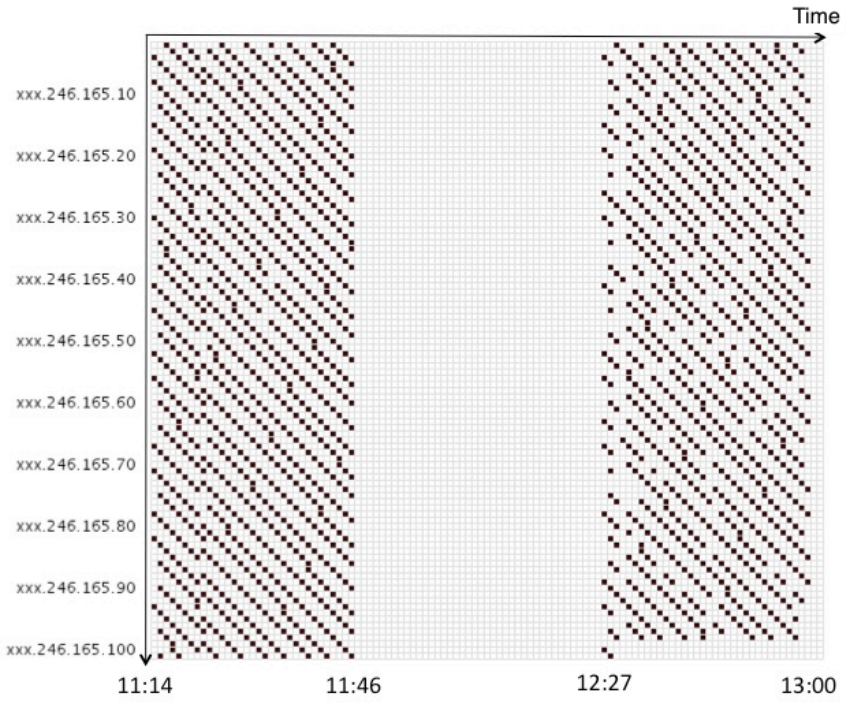


Figure 3.15: Case II: Change of target IP addresses in time series.

3.5 Discussion

3.5.1 Growth of DNS Reflection Attacks

The number of DNS queries that the DNS honeypots observed had changed from 189 queries in a day at the beginning of October 2012 to 340 thousand queries in a day in October 2013. The number of the queries is different from day to day, but the average number of queries has increased approximately 1800 times in a year. It is difficult for us to estimate the global trends of DNS reflection attacks only from the results of these two DNS honeypots. However, these results show that DNS reflection attacks had become a serious threat on the Internet in 2013.

3.5.2 Comparison with Darknet Sensor

In this section, we compare the number of DNS queries between the DNS honeypots and a darknet sensor operated by NICTER [77]. A darknet is unused IP address space (i.e. no legitimate users in the network) on the Internet. By comparing the number of these queries, we can examine the effect of the presence of DNS honeypots that work as an open resolver. In this experiment, we used a darknet sensor which monitors a /16 network (i.e.

Table 3.4: Comparison of DNS queries between DNS honeypots and darknet sensor.

	DNS-HONEY1 (1 addr.)	DNS-HONEY2 (1 addr.)	/16 DARKNET (per addr.)
# of DNS queries (31 days)	14,298,706	6,841,852	380
# of DNS queries (per day)	461,249	220,705	12

65,536 IP addresses) on the Internet, and the sensor does not respond to any queries (i.e. the sensor works as a blackhole sensor).

Table 3.4 shows the number of DNS queries that the DNS honeypots and the darknet sensor observed in October 2013. We used the darknet data provided via NONSTOP [78].

The darknet sensor observed approximately 25 million DNS queries in 31 days. DNS queries were sent to each IP address averagely, and the number of DNS queries that a single IP address observed is 380 packets in 31 days on average, 12 packets in a day. On the other hand, the DNS honeypots that work as an open resolver observed several hundreds of thousands of DNS queries per day during October. From this result, we can observe many malicious activities such as DNS reflection attacks by operating DNS honeypots.

3.5.3 FQDNs used for DNS Reflection Attacks

The FQDNs used for DNS reflection attacks had high amplification factors compared to the popular FQDNs (Table 3.3). The FQDNs include legitimate FQDNs, such as isc.org, ripe.net, and doc.gov, but some FQDNs do not seem to be used for a legitimate purpose. These FQDNs are not only queried a lot, but also had a big size of response because they held more than two hundreds of "A" records or a large size of "TXT" record. Further, these FQDNs were not indexed by web search engines such as Google, and we could not find any legitimate organizations related to the FQDNs. From these results, we believe that these FQDNs were registered by attackers to abuse them in DNS reflection attacks.

3.5.4 Features in Packet Headers

As we show in Section 3.3.3, ID and TTL in IP header, source port number in UDP header, and ID in DNS header are heavily biased. We analyzed these values and found that some attackers used fixed or continuous values in these fields. By continuing the analysis of these features, it is expected that we can identify or classify programs that launch DNS reflection attacks such as malware families and DDoS attack tools.

3.5.5 Effect of Traffic Restriction and IP Churning

In the experiments, we restricted outgoing traffic up to 1 pps per IP address in order not to be involved in attacks. We are not sure if this restriction affects the results or not, but we believe that some attackers do not mind the rate limiting because many DNS queries were observed in spite of this limitation. However, as this technology widely spreads, some attackers might try to evade DNS honeypots. Therefore, we will take care of the adjustment of "Observability" and "Safety" in the future.

As described in Section 3.3.1, the IP addresses of the DNS honeypots had changed nine times and five times respectively. Just after these changes, the honeypots did not observe DNS reflection attacks for a while. However, the honeypots stared to observe DNS reflection attacks in a few days after the IP address changed. This means that attackers look for open resolvers regularly for DNS reflection attacks on the Internet.

3.6 Summary

In this chapter, we propose DNS honeypot to observe malicious activities that abuse DNS servers on the Internet, and we confirm that DNS honeypot can observe DNS reflection attacks. From a long-term observation using two DNS honeypots, we reveal that the threat of DNS reflection attacks had become serious in 2013, and we show the trends and characteristics of DNS reflection attacks, such as victims, abused domain names, and features in packet headers.

Chapter 4

Correlation Analysis between DNS Honeypot and Darknet for Proactive Countermeasure

4.1 Introduction

In Chapter 3, we propose DNS honeypot to observe DNS reflection attacks. DNS honeypot is a decoy DNS cache server that works as an open resolver, and we have analyzed DNS reflection attacks using DNS honeypots. When we analyze traffic related to DNS reflection attacks, it is important to grasp the trends of not only DNS reflection attacks but also scans that attackers conduct in order to look for open resolvers. However, DNS honeypot requires high operational costs as a DNS cache server. Therefore, DNS honeypot is not suitable for a large-scale monitoring to grasp the overall trends of scan activities.

In this chapter, we analyze the correlation of DNS queries between DNS honeypots and a darknet sensor which monitors a /16 network of IPv4 space. A darknet is unused IP address space, and its sensor is suitable for a large-scale monitoring [79] [80] [81] [82]. As a result of comparing DNS queries that the two DNS honeypots and the darknet sensor observed during six months, we confirm that scans which use the same FQDNs as DNS reflection attacks can be observed on the Internet.

The contribution of this chapter is that we analyze the correlation of DNS queries that DNS honeypots and a darknet sensor observe and reveal the scan activities that attackers conduct before launching DNS reflection attacks. We believe that this knowledge will lead to proactive countermeasures against DNS reflection attacks such as the blacklisting of domain names abused for the attacks.

The rest of this chapter is organized as follows. Section 4.2 explains the experiments and observation results of the DNS honeypots and the darknet

Table 4.1: Observation environments of DNS honeypots and darknet sensor.

(a) DNS honeypots.

	DNS-HONEY1	DNS-HONEY2
Location	Japan	
ISP	ISP-A	ISP-B
Function	Open Resolver	
# of IP addr.	1[a]	
Observation period	from June 1st to November 31st, 2013	
# of days	182 days	
Rate limiting	1 pps	

(b) Darknet sensor.

	DARKNET (operated by NICTER[77])
Location	Japan
Function	Blackhole Sensor
# of IP addr.	65536 (/16 network)
Observation period	from June 1st to November 31st, 2013
# of days	173 days [b]

[a] IP addresses are assigned by ISPs dynamically.
[b] There is no data for the rest of nine days because of the system maintenance.

sensor. Section 4.3 analyzes the correlation of DNS queries between the two DNS honeypots and the darknet sensor. Section 4.4 discusses the results, and Section 4.5 summarizes this chapter.

4.2 Experiments and Results

4.2.1 Experiments

In this chapter, we analyze DNS queries that two DNS honeypots and a /16 darknet sensor observed. Table 4.2a and Table 4.2b show the overview of the environments of each observation system.

The two DNS honeypots (DNS-HONEY1 and DNS-HONEY2) were operated in different ISP networks in Japan, and they restricted outgoing packets up to 1 pps (packets per second) in order not to be involved in attacks. The darknet sensor (DARKNET) provided by NICTER [77] via NONSTOP [78] monitored a /16 network (i.e. 65,536 IP addresses) and worked as a blackhole sensor (i.e. the sensor does not respond to any packets). Note that we excluded the darknet data for nine days from this analysis.

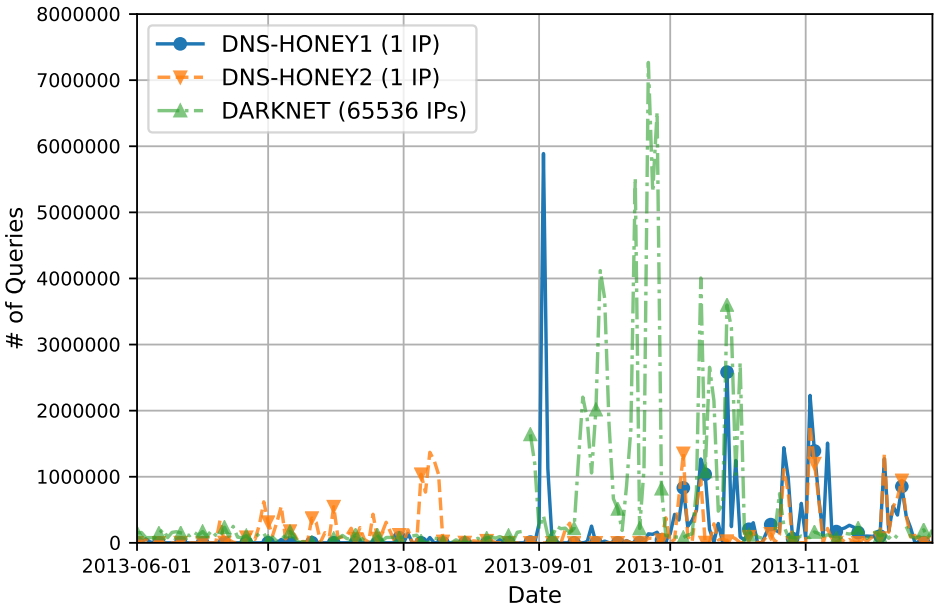


Figure 4.1: Number of DNS queries observed by DNS honeypots and darknet sensor.

4.2.2 Results

Table 4.2 shows the overview of DNS queries that the DNS honeypots and the darknet sensor observed during the observation period, and Figure 4.1 shows the daily change in the number of the DNS queries.

The DNS honeypots observed more than 64 million DNS queries in total, more than 300 thousand DNS queries per day on average during the observation period of 182 days. On the other hand, the darknet sensor monitors more than 89 million DNS queries in total, eight DNS queries in a day per IP address.

The DNS honeypots observed more than ten thousand IP addresses, but the darknet sensor observed 6,867 IP addresses in total. Thus, the number of DNS queries and source IP addresses that the darknet sensor observed are smaller than that of the DNS honeypots. This is because a darknet sensor observes only scan activities, whereas DNS honeypot observes not only scans but also DNS reflection attacks.

In contrast, the number of FQDNs that the darknet sensor observed is larger than that of the DNS honeypots. This is because some of the FQDNs contain strings related to their IP addresses (e.g. FQDNs used for reverse lookup), and these FQDNs raise the number of FQDNs observed by the darknet sensor.

Table 4.2: Observation results of DNS honeypots and darknet sensor.

(a) DNS honeypots.

	DNS-HONEY1 (1 addr.)	DNS-HONEY2 (1 addr.)
# of DNS queries (182 days)	34,838,637	29,510,478
# of DNS queries (1 day)	191,421	162,145
# of source IP addr. (182 days)	29,129	12,948
# of FQDNs (182 days)	1,369	431

(b) Darknet sensor.

	Darknet (65,536 addr.)	Darknet (1 addr. average)
# of DNS queries (173 days)	89,408,057	1,364
# of DNS queries (1 day)	516,810	8
# of source IP addr. (173 days)	6,867	-
# of FQDNs (173 days)	488,678	-

4.2.3 FQDNs used for DNS Reflection Attacks

Table 4.3 shows TOP-10 FQDNs that the DNS honeypots observed. This table shows that the amplification factors of these FQDNs are bigger than the popular FQDNs shown in Table 3.4a. In addition, some attackers used legitimate FQDNs such as isc.org [83] and ripe.net [84] for DNS reflection attacks. The other FQDNs such as pkts.asia and aa3247.com held hundreds of DNS resource records or a big size of TXT record, and we could not find any evidence that some legitimate organizations had these FQDNs. Therefore, we believe these FQDNs were prepared for DNS reflection attacks by attackers.

In the next section, we analyze these FQDNs which attackers prepared — we call them "malicious" FQDNs — to reveal the relationship between scan activities and DNS reflection attacks.

Table 4.3: FQDNs used for DNS reflection attacks.

FQDN	Type	# of DNS queries[1]	AF (%)[2]	Response[3]	Response code (January 22th, 2014)	Benign / Malicious
isc.org	ANY	14,414,573	4541%	various records	NOERROR	Benign
pkts.asia	ANY	12,262,517	5070%	245 records	NXDOMAIN	Malicious
anonsc.com	ANY	7,323,906	-[4]	201 records	NXDOMAIN	Malicious
aa3247.com	A	3,790,906	5379%	256 records	NXDOMAIN	Malicious
babywow.co.uk	ANY	3,772,660	5488%	246 records	NOERROR (small response[5])	Malicious
eschenemnogo.com	ANY	3,217,076	4739%	246 records	- (no response[6])	Malicious
ym.rctrhash.com	ANY	2,396,101	-[4]	large TXT record	NXDOMAIN	Malicious
a.packetdevil.com	ANY	2,396,055	4723%	252 records	SERVFAIL	Malicious
irlwinning.com	ANY	2,279,340	4778%	245 records	NOERROR (small response[5])	Malicious
fkfkfkfa.com	ANY	2,201,520	4900%	245 records	NXDOMAIN	Malicious

[1] The sum of the number of queries that DNS-HONEY1 and DHS-HONEY2 observed.
[2] Amplification factor (AF) is calculated in the same formula as 3.1.
[3] As of the time when DNS reflection attacks were observed.
[4] Undefined because we could not estimate the response size.
[5] These FQDNs do not seem to be owned by attackers, but seem to be parked by domain registrars.
[6] Undefined because we could not receive answers from authoritative nameservers.

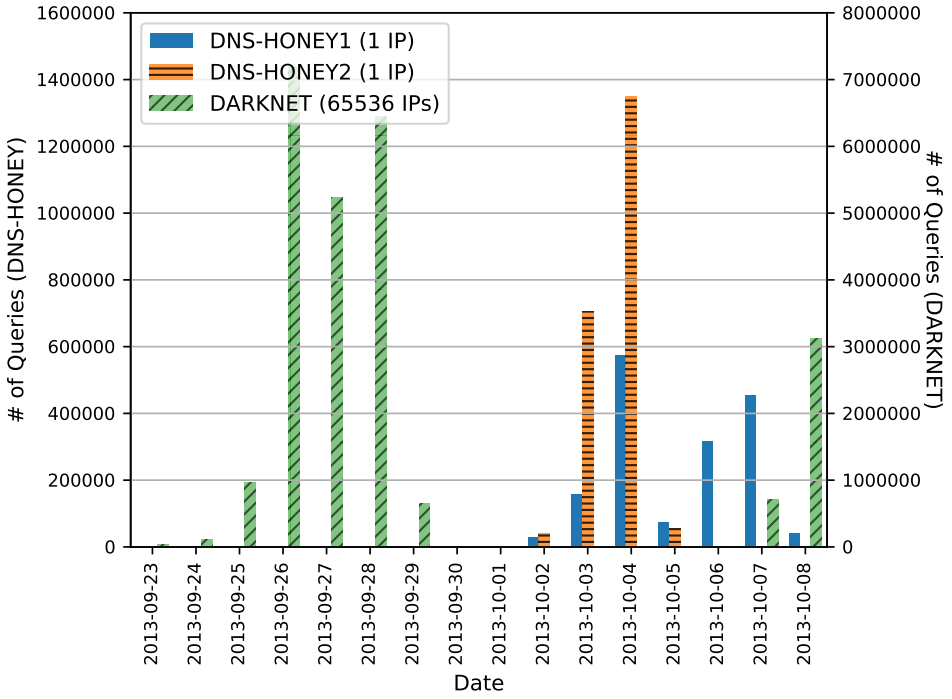


Figure 4.2: Case I: Number of aa3247.com queries.

4.3 Correlation Analysis

In this section, we analyze the correlation of DNS queries between the DNS honeypots and the darknet sensor. The purpose of this analysis is to analyze the correlation between DNS reflection attacks and scan activities focusing on FQDNs.

4.3.1 Case Studies

In this section, we analyze the correlation of three FQDNs (aa3247.com, pkts.asia, and bitstress.com) as case studies.

4.3.1.1 Case I: aa3247.com

DNS queries of aa3247.com were observed approximately 380 million times by the two DNS honeypots during the analysis period. The FQDN held 256 IP addresses and its amplification factor was about 54.

Figure 4.2 shows the number of DNS queries of aa3247.com that the DNS honeypots and the darknet sensor observed. Scans of aa3247.com were observed on September 23, 2013, for the first time by the darknet sensor. After that, the darknet sensor observed a lot of DNS queries of the FQDN

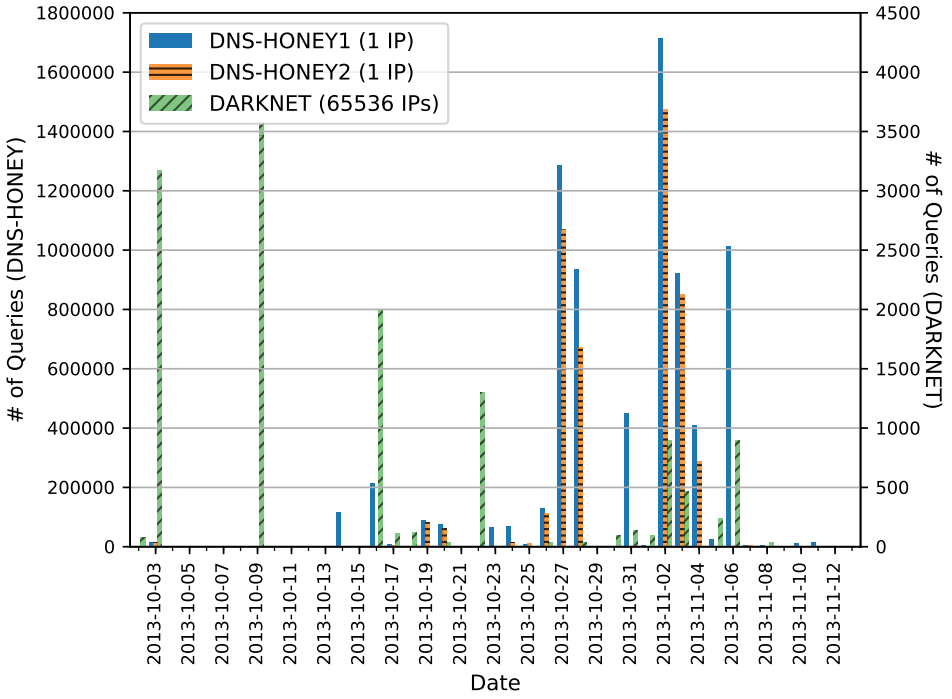


Figure 4.3: Case II: Number of pkts.asia queries.

for a week. On the other hand, the DNS honeypots observed DNS reflection attacks using aa3247.com on October 2, after nine days from the first scan, and the number of queries reached its peak on October 4, after 11 days from the first scan.

4.3.1.2 Case II: pkts.asia

DNS queries of pkts.asia were observed approximately 12 million times by the two DNS honeypots during the analysis period. The FQDN held 245 IP addresses and its amplification factor was about 50.

Figure 4.3 shows the number of DNS queries of pkts.asia that the DNS honeypots and the darknet sensor observed. Scans of pkts.asia were observed on October 2, 2013, for the first time by the darknet sensor. The next day, the DNS honeypots observed DNS reflection attacks using pkts.asia. After that, a large number of scans querying pkts.asia were observed every 5-6 days by the darknet sensor. The number of DNS reflection attacks using pkts.asia increased after October 14, and the number of queries reached its peak on November 2, after 31 days from the first scan.

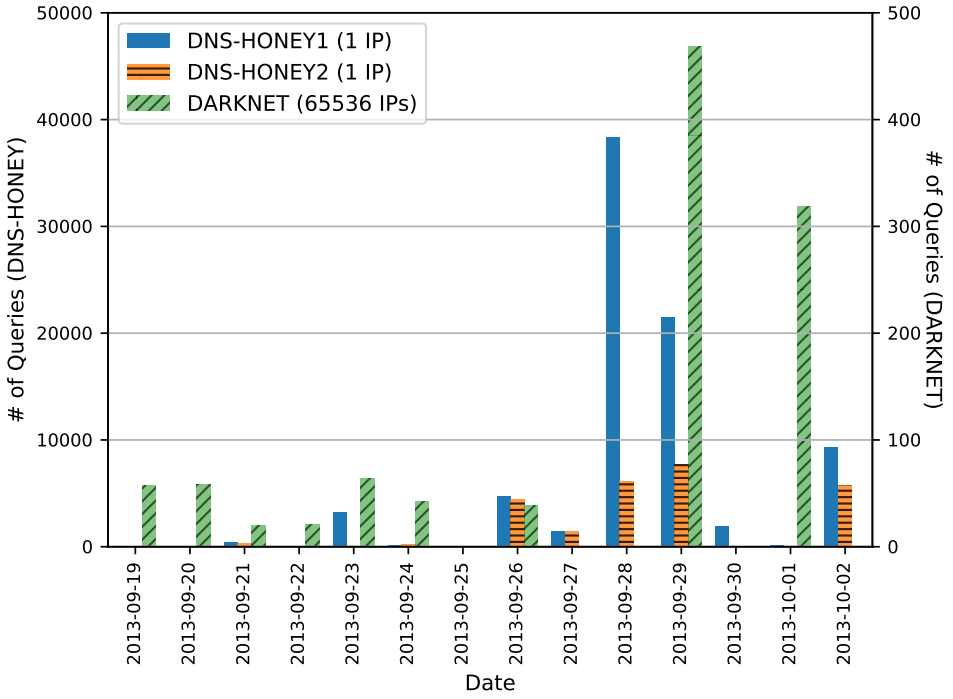


Figure 4.4: Case III: Number of bitstress.com queries.

4.3.1.3 Case III: bitstress.com

DNS queries of bitstress.com were observed approximately 170 thousand times by the two DNS honeypots during the analysis period. The FQDN held 242 IP addresses and its amplification factor was about 48.

Figure 4.4 shows the number of DNS queries of bitstress.com that the DNS honeypots and the darknet sensor observed. Scans of bitstress.com were observed on September 19, 2013 for the first time by the darknet sensor. After that, the darknet sensor observed continuous DNS queries of the FQDN. On the other hand, the DNS honeypots observed DNS reflection attacks using bitstress.com on September 23, after four days from the first scan, and the number of queries reached its peak on September 28, after 11 days from the first scan.

4.3.2 Number of Days from Scans to Attacks

In this section, we analyze malicious FQDNs that the DNS honeypots observed more than one thousand times during the analysis period. These FQDNs are considered to be prepared for DNS reflection attacks by attackers.

We find 33 FQDNs in total during this period and we analyze them in the same way as the case studies in Section 4.3.1.

Table 4.4: Observation date of aa3247.com, pkts.asia, and bitstress.com.

(a) First scan date.

FQDN	First scan date
aa3247.com	2013-09-23
pkts.asia	2013-10-02
bitstress.com	2013-09-19

(b) First attack date.

FQDN	First attack date	Days from (a)
aa3247.com	2013-10-02	9 days
pkts.asia	2013-10-03	1 day
bitstress.com	2013-09-23	4 days

(c) Attack peak date.

FQDN	Attack peak date	Days from (a)
aa3247.com	2013-10-04	11 days
pkts.asia	2013-11-02	31 days
bitstress.com	2013-09-28	9 days

1. # of days from the first scan to the first attack
   The number of days from the date when a scan of the FQDN was observed for the first time by the darknet sensor to the date when DNS reflection attacks using the FQDN were observed for the first time by the DNS honeypots.

2. # of days from the first scan to the peak
   The number of days from the date when a scan of the FQDN was observed for the first time by the darknet sensor to the date when the number of DNS queries of the FQDN reached its peak by the DNS honeypots.

Table 4.5 shows the distribution of the two types of days on the 33 FQDNs. As a result of the analysis, 22 out of 33 FQDNs (66.7%) were observed by the darknet sensor one or more days before DNS reflection attacks were observed by the DNS honeypots. In addition, 27 out of 33 FQDNs (81.8%) were observed by the darknet sensor one or more days before the number of DNS queries of the FQDNs reached their peak. From these results, before DNS reflection attacks are observed by DNS honeypots, scanning activities using the same domain name as attacks can be observed by a darknet sensor.

Table 4.5: Number of days from first scans to attacks.

(a) From first scans to first attacks.

# of days	# of FQDNs	%
0 day (the same day)	4	12.1%
1 day	5	15.2%
2 – 7 days	7	21.2%
8 – 30 days	6	18.2%
more than 30 days	4	12.1%
scans after attacks	3	9.1%
no scans in darknet	4	12.1%

(b) From first scans to peaks of attacks.

# of days	# of FQDNs	%
0 day (the same day)	1	3.0%
1 day	4	12.1 %
2 – 7 days	9	27.3%
8 – 30 days	7	21.2%
more than 30 days	7	21.2%
scans after peak	1	3.0%
no scans in darknet	4	12.1%

4.4 Discussion

In this section, we discuss the analysis results and proactive countermeasure against DNS reflection attacks using the knowledge shown in Section 4.3.

4.4.1 FQDNs Prepared by Attackers

FQDNs that we determined that attackers prepared for DNS reflection attacks had high amplification factors when they were used for attacks. However, as of January 22, 2014, the responses of the FQDNs had changed: some FQDNs did not exist (NXDOMAIN), and others were parked by registrars. This is probably because attackers tend to change the FQDNs used for DNS reflection attacks in a short period to avoid the detection. This tendency matches with the characteristics of other malicious FQDNs such as C&C servers of botnets [85].

4.4.2 Purpose of Scans

From the result in Section 4.3, 29 out of 33 FQDNs used for DNS reflection attacks were also observed by the darknet sensor. In this section, we discuss

the reason why attackers conduct scans by FQDNs used for DNS reflection attacks.

In order to conduct DNS reflection attacks, attackers need to know IP addresses of open resolvers to abuse as reflectors. However, some open resolvers may stop their service or their IP addresses may change because IP addresses are assigned dynamically if they are in ISP networks. Therefore, attackers need to conduct scans on the Internet to update the list of open resolvers regularly.

In addition, attackers need to check if an FQDN that they prepare can be resolved by open resolvers or not before they conduct attacks. This is because some DNS cache servers do not support big size of responses in UDP and/or reject some of DNS queries. For example, if DNS cache servers do not support EDNS0 (Extension Mechanisms for DNS) [71], they cannot send responses more than 512 octets in UDP. Therefore, these resolvers are not suitable for DNS reflection attacks. Besides, some public DNS cache servers such as Google Public DNS [86] restrict the response of some DNS queries such as isc.org (ANY), and these DNS cache servers are difficult to abuse.

For the above reasons, when attackers gather the IP addresses of open resolvers by scans, they use the same FQDNs as DNS reflection attacks.

4.4.3 FQDNs Not Observed by Darknet

As described in the previous section, 29 out of 33 FQDNs used for DNS reflection attacks were observed by the darknet sensor. However, the rest of four FQDNs were not observed by the darknet sensor. We assume two reasons.

First, attackers conducted scans using another FQDN whose amplification factor was high. In this case, the darknet sensor cannot observe FQDNs and it is difficult to find FQDNs used for DNS reflection attacks before attacks. However, attackers cannot test if the FQDN is resolvable by open resolvers, and therefore, attackers are responsible for the failure of the attacks.

Second, attackers conducted scans using the same FQDNs as attacks, but they did not scan the network that the darknet sensor located because attackers do not need to scan the whole of networks on the Internet. In this case, we cannot observe scans by the darknet sensor we used. But by analyzing the other darknet sensors, we may be able to improve the observability of FQDNs used for DNS reflection attacks.

4.4.4 Approaches to Proactive Countermeasure

The result of analysis described in this chapter shows that we might be able to detect FQDNs used for DNS reflection attacks from scan activities before the FQDNs are used for attacks. These FQDNs have high amplification factors because they hold many resource records or a large TXT record, and scans

using the FQDNs are widely observed on the Internet. Therefore, if we find FQDNs which have high amplification factors and are scanned widely on the Internet, we can extract FQDNs used for DNS reflection attacks from scan activities.

An algorithm to detect the FQDNs and its evaluation are the future challenges, but it is effective to use this knowledge and build the framework to take countermeasures against DNS reflection attacks.

The rest of this section explains proactive countermeasures against DNS reflection attacks using this knowledge. First, registrars and law enforcements can revoke FQDNs that can be used for DNS reflection attacks. Besides, administrators of DNS cache servers can block the FQDNs and mitigate the effect of attacks by changing the configuration. This is effective when administrators cannot close their DNS cache servers for some reasons or some open resolvers work as proxies to other DNS cache servers.

4.5 Summary

In this chapter, we analyze the correlation of DNS queries between two DNS honeypots and a darknet sensor. As a result of comparison of DNS queries that the DNS honeypots and the darknet sensor observed, we confirm that scans which use the same FQDNs as DNS reflection attacks can be observed on the Internet.

The result of this chapter shows that FQDNs can be detected before DNS reflection attacks focusing on scanning activities observed on the Internet. This knowledge can be expected to take proactive countermeasures against DNS reflection attacks using scan information.

Chapter 5

Observation of DRDoS Attacks using DRDoS Honeypots

5.1 Introduction

In recent years, Distributed Reflection DoS (DRDoS) attacks have become a serious threat on the Internet. The attacks interfere with services by sending a large number of packets via open servers which work in an inappropriate setting on the Internet. The volume of the traffic generated by DRDoS attacks is different by attacks, but it is reported that the attack against Spamhaus [8] in March 2013 reached 300 Gbps [10] and the attack against OVH [11] in February 2014 reached 400 Gbps [12]. Recently, DDoS provider services called "Booter" or "Stresser" have emerged [14] [15], and users who do not have the knowledge of DDoS attacks can easily launch DDoS attacks. Besides, hacker groups such as Anonymous, Lizard Squad, DD4BC, and Armada Collective utilize DRDoS attacks to achieve their goals. Thus, the threat of DRDoS attacks is getting more and more serious.

In Chapter 3, we propose DNS honeypot to observe DNS reflection attacks and confirm that DNS honeypot can observe DNS reflection attacks. In this chapter, we enhance DNS honeypot to DRDoS honeypot in order to observe not only DNS reflection attacks but also other types of DRDoS attacks, and we analyze the trends and characteristics of DRDoS attacks that the DRDoS honeypots observed during half a year from January to June in 2015. As a result, six DRDoS honeypots observed 725,703 attacks during the period. We analyzed these attacks and found the following facts: 50% of the attacks lasted for less than five minutes, 80% of victims aggregated by the IP address were attacked only once in half a year, and 33% of the attacks, on the contrary, went to only ten Autonomous Systems (ASes), etc.

The rest of this chapter is organized as follows. First, Section 5.2 describes

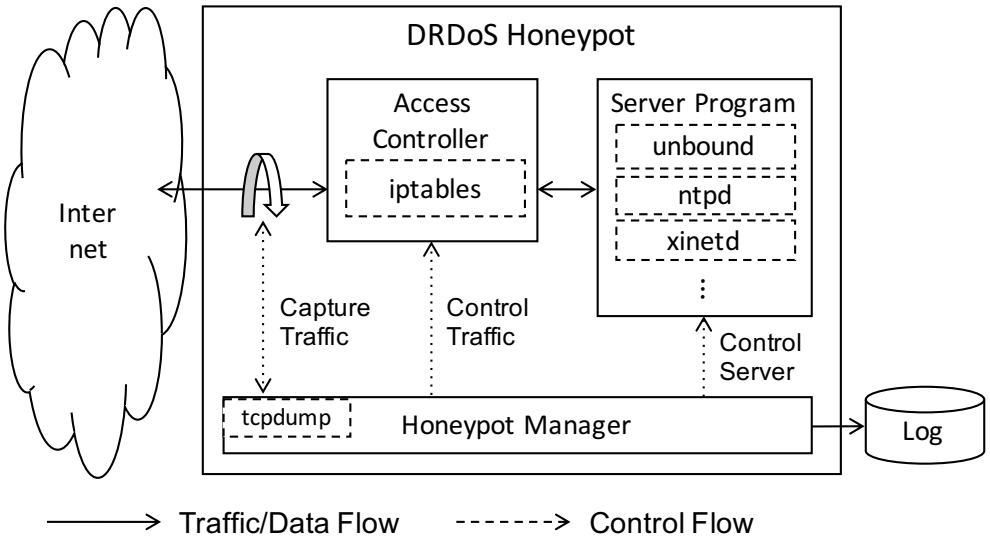


Figure 5.1: Architecture and implementation of DRDoS honeypot.

the architecture and implementation of DRDoS honeypot. Then, Section 5.3 explains the definition of DRDoS attacks in this experiment, and reports the operation of the DRDoS honeypots. Section 5.4 analyzes the DRDoS attacks that six DRDoS honeypots observed in the first half of 2015. Section 5.5 discusses the analysis results, and Section 5.6 summarizes this chapter.

5.2 DRDoS Honeypot

In this section, we improve DNS honeypot described in Chapter 3 to DRDoS honeypot that observes not only DNS reflection attacks but also other types of DRDoS attacks.

The concept of the DRDoS honeypot is the same as the DNS honeypot. Therefore, in this section, we omit the explanation of the requirements of the DRDoS honeypot, and start the description of the architecture of the DRDoS honeypot (See Section 3.2.1 for the requirements).

5.2.1 Architecture

DRDoS honeypot is a decoy reflector to observe DRDoS attacks from the reflector's point of view. Figure 5.1 shows the architecture and implementation of the DRDoS honeypot. The DRDoS honeypot consists of three components in the same way as the DNS honeypot.

Server Programs

"Server Programs" play roles in responding to incoming queries. Here,

Table 5.1: List of services supported by DRDoS honeypot.

Service	Port	Implementation
QOTD	17/UDP	quoted [87]
CHG	19/UDP	xinetd [88]
DNS	53/UDP	BIND [67], Unbound [89]
NTP	123/UDP	NTP Project [90]
SNMP	161/UDP	Net-SNMP [91]
SSDP	1900/UDP	Handmade script

we utilize not only a DNS server but also other types of servers that can be abused for DRDoS attacks (e.g. NTP server, SSDP server).

Access Controller
"Access Controller" is located in between the Internet and "Server Programs," and controls the traffic of the servers when the servers are abused by attackers.

Honeypot Manager
"Honeypot Manager" controls "Server Programs" and "Access Controller," and outputs logs of DRDoS honeypots.

The data collected by the DRDoS honeypots are transferred to the analyzer so as to analyze the details of DRDoS attacks (See Section 3.2.2).

5.2.2 Implementation

In the current implementation of the DRDoS honeypot as of October 2014, we prepare a machine which installs Ubuntu [66] for each observation point. On the Ubuntu machine, iptables [68] works as "Access Controller," and handmade shell scripts work as "Honeypot Manager."

The current DRDoS honeypot supports six protocols which can be abused for DRDoS attacks: QOTD (17/udp), CHG (19/udp), DNS (53/udp), NTP (123/udp), SNMP (161/udp) and SSDP (1900/udp). Table 5.1 shows the list of supported services and implementations we install on each machine. The traffic data are captured by tcpdump [69], and they are saved as a libpcap file format.

5.3 Experiments

The traffic that DRDoS honeypots observe includes not only DRDoS attacks but also scans and other malicious activities. Furthermore, when a DRDoS attack starts, the DRDoS honeypot receives so many packets that it is difficult to analyze the traffic by the packet.

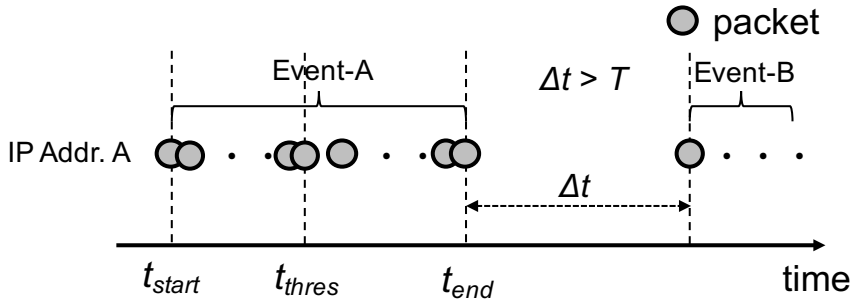


Figure 5.2: Event definition.

In this section, we first describe the definition of an "event" to make a group of packets. Then, we outline the operation of the DRDoS honeypots.

5.3.1 Attack Definition

First, when a DRDoS honeypot receives a packet, the packet is grouped by the pair of honeypot ID, abused service, source IP address (i.e. a victim of an attack). The packets in a group are sorted by the arrival time. If the time difference Δt between the two packets is less than the threshold T, then the packets are considered to be the same event, and otherwise, the two packets are considered as a different event. Lastly, if the number of packets in the group exceeds the threshold N_{attack}, then the group is considered as an attack.

In this chapter, we tentatively set the thresholds as follows: $T = 60$ [seconds] and $N_{attack} = 100$ [packets]. Although we need to verify the validity of these thresholds, we believe that these thresholds work well to extract DRDoS attacks and exclude scans and other types of attacks.

5.3.2 Honeypot Operation

We deploy seven DRDoS honeypots in ISP networks in Japan as of October 2016. We started observation on October 7th, 2012 and we have gradually increased the number of DRDoS honeypots and the supported services to observe more DRDoS attacks (Table 5.2). Note that H01 discontinued observation on October 9th, 2015 and H08 was added instead of H01 on November 9th, 2015.

These DRDoS honeypots run under ISP networks in Japan, and their IP addresses are assigned by ISPs dynamically. The intervals of re-assignment of the IP addresses are various depending on ISPs and the situation, but the DRDoS honeypots keep the same IP addresses for a few months on average.

Table 5.2: Deployed dates of DRDoS honeypots.

Honey ID	ISP	Deployed date	Added date					
			QOTD	CHG	DNS	NTP	SNMP	SSDP
H01[1]	ISP-A	2012-10-06	2014-09-25	2013-07-26	2012-10-06	2014-09-25		
H02	ISP-B	2013-05-13	-	-	2013-05-13	-	-	-
H03	ISP-C	2014-05-13	2014-05-13				2014-09-17	2014-10-03
H04	ISP-D	2014-05-13	2014-05-13				2014-09-17	
H05	ISP-E	2014-05-10	2014-05-10				2014-10-18	
H06	ISP-F	2014-05-10	2014-05-10				2014-10-18	
H07	ISP-F	2014-05-10	2014-05-10				2014-10-18	
H08	ISP-G	2015-11-09	2015-11-09					

[1] Discontinued on 2015-10-09.

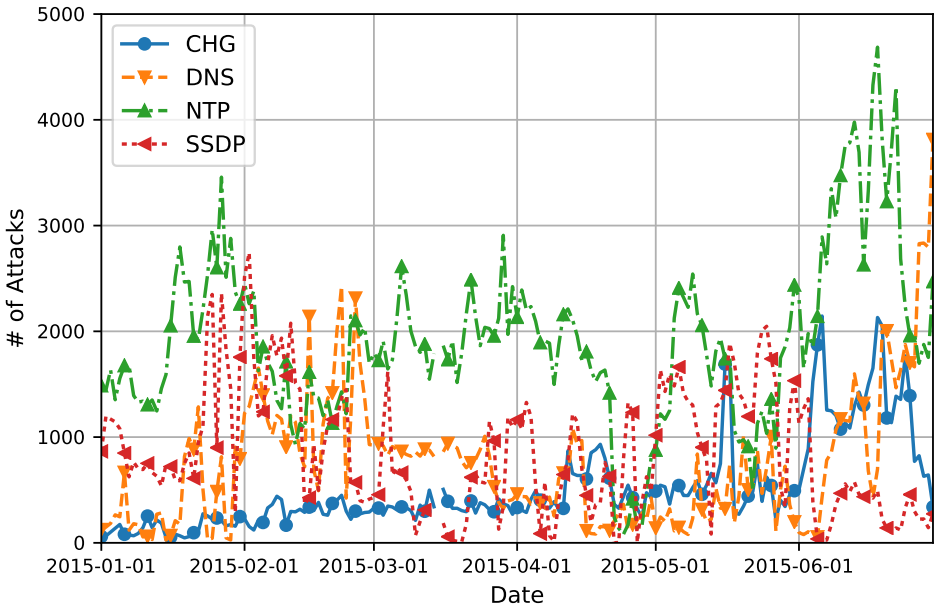


Figure 5.3: Number of DRDoS attacks observed by DRDoS honeypots.

5.4 Analysis

In this section, we analyze the observation results of DRDoS honeypots in order to grasp the trend and characteristics of DRDoS attacks in the wild.

5.4.1 Dataset

In this section, we analyze DRDoS attacks that six out of the seven DRDoS honeypots observed during half a year (181 days) from January to June in 2015. We excluded H02 from this analysis for brevity because H02 supported only DNS.

Table 5.3 shows the overview of the observation results and Figure 5.3 illustrates the number of DRDoS attacks in a day. The DRDoS honeypots observed 725,703 attacks during 181 days. The number of attacks per protocol was as follows: 37 QOTD attacks (0.00005%), 92,602 CHG attacks (13%), 133,963 DNS attacks (18%), 344,730 NTP attacks (48%), 400 SNMP attacks (0.0006%), 153,971 SSDP attacks (21%).

The DRDoS honeypots observed approximately four thousand DRDoS attacks every day, and especially, 1,904 NTP reflection attacks in a day on average. Since DRDoS attacks which abuse QOTD and SNMP were hardly observed, in this section, we analyze DRDoS attacks that abuse the following four protocols: CHG, DNS, NTP, SSDP.

Table 5.3: Observation results of DRDoS honeypots.

Honey ID	Days	Changes of IP addr.	# of attacks						
			QOTD	CHG	DNS	NTP	SNMP	SSDP	Total
H01	179	5	16	25,713	35,029	159,535	9	40,845	261,131
H03	180	3	20	39,563	57,204	173,027	7	64,284	334,085
H04	161	5	4	17,448	30,130	118,740	8	46,577	212,903
H05	179	0	26	45,807	46,910	206,384	391	33,948	333,440
H06	178	0	17	45,457	33,538	198,202	8	13,908	291,113
H07	178	2	14	53,591	51,413	170,390	6	41,280	316,680
Total[1]	181	-	37	92,602	133,963	344,730	400	153,971	725,703

[1] The values in "Total" line are not the sum of each honeypot (H01-H07) because each honeypot sometimes observes the same attacks simultaneously and these same attacks are merged in this analysis.

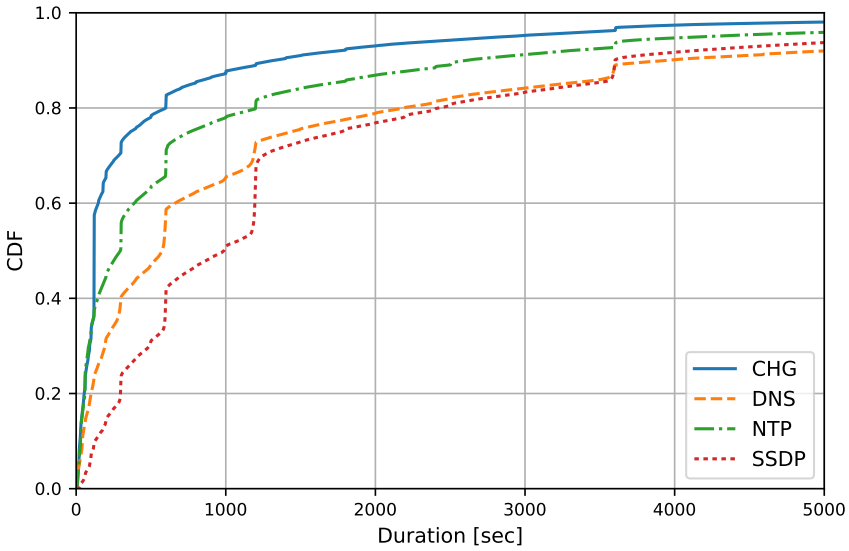


Figure 5.4: CDF of attack duration.

5.4.2 Attack Duration

Figure 5.4 shows the distribution of attack duration. The attack duration was slightly different by each service, but the exact duration such as 300, 600, 900, 1200 seconds is popular for all the services. When comparing each service, the attack duration of CHG is the shortest and that of SSDP is the longest. Looking at all the services, 18% of the attacks lasted only for one minute or less, and 48 % of the attacks lasted for less than five minutes, and only 8% of the attacks lasted for more than one hour.

5.4.3 Victim Services

During the observation period, the DRDoS honeypots observed attacks that the source port numbers are fixed to the known port numbers such as 22 (SSH), 80 (HTTP), and 443 (HTTPS). In particular, 250,330 of the attacks (35%) were sent to port 80 (HTTP), 13,922 attacks (1.9%) against port 3704 (Xbox), 8,193 attacks (1.1%) against port 53 (DNS), and 5,793 (0.8%) attacks against port 25565 (Minecraft).

This result does not always mean that these services are actually targeted, but it gives us a hint about victim services.

5.4.4 Honeypot Coverage

Figure 5.5 shows how many honeypots observed the DRDoS attacks. Approximately 80 % of NTP reflection attacks were observed by multiple

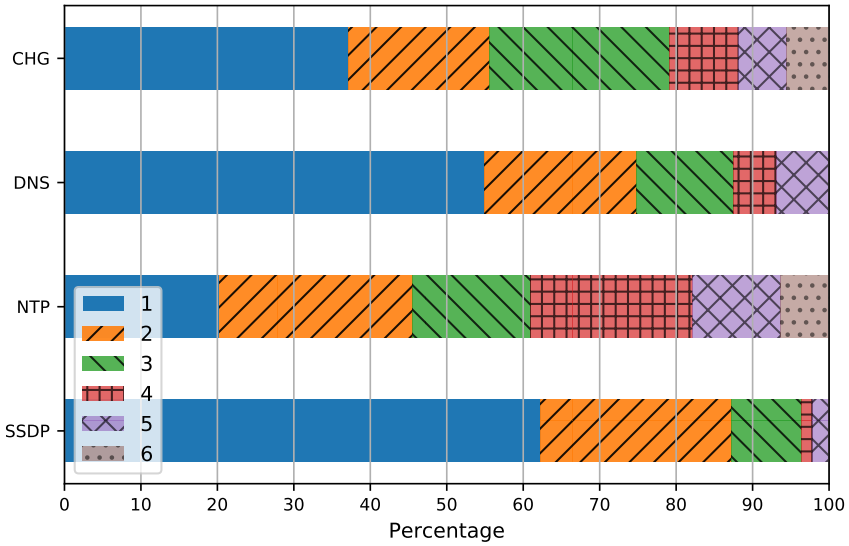


Figure 5.5: Coverage of DRDoS honeypots.

DRDoS honeypots. On the other hand, only 40 % of DNS reflection attacks were observed by multiple DRDoS honeypots.

This result means that the DRDoS honeypots do not observe all DRDoS attacks on the Internet and we need to deploy more honeypots in order to improve the coverage.

5.4.5 Attack Repetition

Figure 5.6 shows the distribution of attack repetition per victim aggregated by the IP address, the /24 network, the /16 network, and the AS respectively.

If we look at attack repetition by the IP address, 80% of the victims received only one attack and only 1.5% of the victims attacked ten or more times in half a year. The attack repetition by the /24 network goes to the same trends as the case by the IP address, but when we aggregate the victim by the /16 network and the AS, more than 50% of the victims received ten or more attacks during this observation period.

5.4.6 Victim Deviation

Table 5.4 shows the rankings of the victims by the IP address, the /16 network, the AS, and the country during 181 days. The most targeted IP address was owned by a company which provided CDN service in the United States, and it was attacked 334 times. When aggregating the victims by the /16 network and the AS, the network that an ICT company owned in China was the most

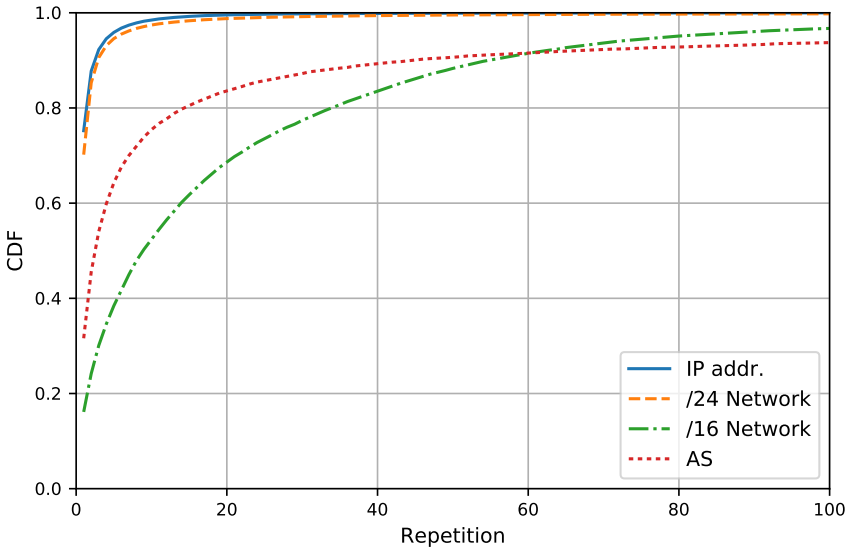


Figure 5.6: CDF of attack repetition.

Table 5.4: Victim Rankings.

(a) IP address.

#	IP address
334	■.31.20.35
333	■.31.103.172
325	■.163.224.34
298	■.28.132.69
297	■.1.1.1

(b) /16 network.

#	/16 network
7,517	■.28.0.0/16
6,117	■.60.0.0/16
4,696	■.231.0.0/16
4,686	■.96.0.0/16
4,564	■.29.0.0/16

(c) AS number.

#	AS number
46,270	AS ■134
34,949	AS ■7963
30,656	AS ■922
30,083	AS ■837
27,165	AS ■6276

(d) Country.

#	Country
214,578	United States
186,609	China
43,524	France
26,899	United Kingdom
26,420	Germany

The parts of the values in this table are masked for anonymity.

targeted. When aggregating the victims by the country, 50% of the attacks were against the United States and China in total.

Table 5.5 shows the ratio, how many attacks the victims occupied by the IP address, the /16 network, and the AS. If we look at the victims by the

Table 5.5: Victim Ratio by IP address, network, and AS.

Target	# of Attacks	# of Targets	Ratio		
			Top10	Top100	Top1000
IP addr.	725,703	398,756	0.4%	1.9%	7.3%
Network (/16)		23,972	6.6%	24.9%	47.9%
AS		10,019	32.9%	66.5%	92.7%

IP address, the TOP-10 of the targeted IP addresses occupied 0.4% of the attacks. However, if we aggregate the victims by the AS, the TOP-10 ASes (0.02% out of all ASes on the Internet) accounted for 32.9% of the attacks and the TOP-100 ASes (0.2% out of all ASes) occupied 66.5%. We need to consider the size of the ASes and the accuracy of the GeoIP database, but these results show that the targets of the DRDoS attacks are heavily biased.

5.4.6.1 Visualization of Victim Deviation using IPv4 Heatmap

A method for visualizing IPv4 space using Hilbert curve is proposed [92]. Mapping IPv4 addresses on the Hilbert curve on a two-dimensional plane is suitable for representing the locality of IP addresses because the IP addresses which is numerically closer distance is mapped to a spatially closer point on the plane.

In this section, we visualize the deviation of victims by the heatmap visualization. We used an open source tool [92] for visualization and set up as follows.

- We depict a /16 network as one pixel and draw IPv4 space in an image of 256 x 256 pixels.
- The color of each pixel represents the number of attacks against the /16 network (black: 0, blue: 1, ... red: 256 or more)

Figure 5.7 shows the result of the visualization. From this figure, we can confirm that the parts of the networks are frequently targeted while many networks on the Internet are attacked.

5.5 Discussion

During the analysis period, the DRDoS honeypots observed approximately four thousand DRDoS attacks in a day. From this result, the DRDoS honeypots work well to observe DRDoS attacks on the Internet.

Although an enormous number of attacks have been observed, many of them have the short duration and most of the targets are attacked only once

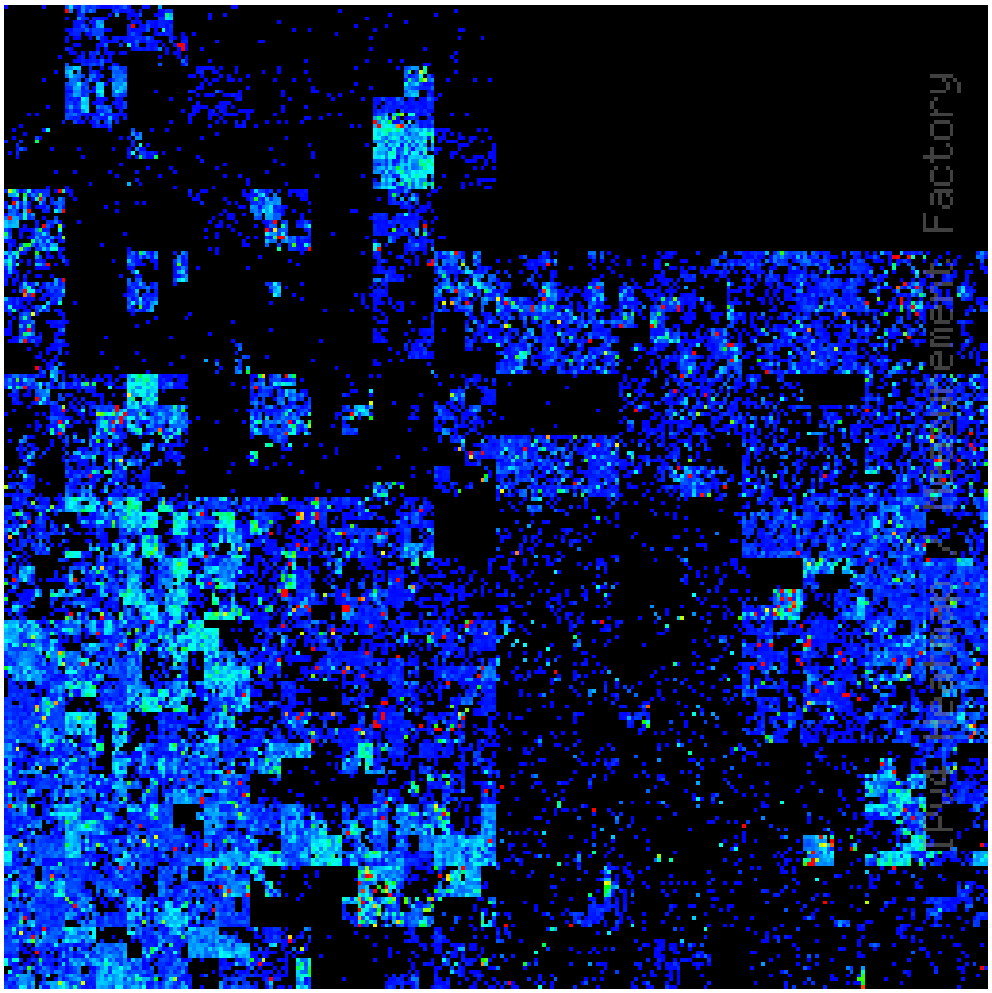


Figure 5.7: Heatmap of victim networks.

in the period. From these results, we speculate that the DRDoS honeypots observed a lot of "test" attacks. In fact, booter services offer conditional DDoS attacks (e.g. short duration, low volume, etc.) for a free or reasonable price, and we believe that these booter services are key factors in raising the number of DRDoS attacks.

In addition, as described in Section 5.4.3, some attacks targeted some specific ports such as 80 (HTTP) and 53 (DNS). We are not sure of the reason, but we believe that some attackers try to evade packet filtering by firewalls and send amplified packets to the target servers.

Further, as shown in Section 5.4.5 and 5.4.6, the victims of the DRDoS attacks are heavily biased. Although the precise evaluation is the future challenges, we believe that the knowledge will help operators of ISPs by sharing the information.

5.6 Summary

In this section, we enhance DNS honeypot to DRDoS honeypot in order to observe DRDoS attacks, and we analyze the attacks that DRDoS honeypots observed during the first half of 2015.

As a result of analysis, we confirm that DRDoS honeypots observed approximately four thousand DRDoS attacks in a day, most of the attacks lasted only for a few minutes, most of the victims by the IP address were targeted only once during the period, and the victims were heavily biased when aggregating the victims by the AS. In particular, when we aggregate victims by the AS, the TOP-10 ASes (0.02% out of all ASes on the Internet) occupied 32.9% of the attacks and the TOP-100 ASes (0.2%) occupied 66.5%.

These results will lead to the better understandings of DRDoS attacks, and by sharing this information, we can help operators of ISPs to understand the trends and characteristics of DRDoS attacks.

Chapter 6

DRDoS Attack Alert System for Real-time Response

6.1 Introduction

Distributed Reflection DoS (DRDoS) attacks have become a major threat on the Internet. In Chapter 5, we propose DRDoS honeypot to observe DRDoS attacks from the reflector's point of view, and we show that DRDoS honeypots can observe many DRDoS attacks in the wild.

In this chapter, we propose DRDoS attack alert system using DRDoS honeypots as a countermeasure against DRDoS attacks. This alert system aims to help network administrators to grasp the situation of attacks accurately and quickly, and the administrators utilize this alert information for real-time responses such as mitigation and recovery. We have been operating this system and providing DRDoS attack alerts to several organizations under an R&D project in Japan. As a result of the operation, we compare attack detection times between the alert system and an ISP's mass traffic detector, and we confirm that the alert system is able to provide accurate and quick alerts to the collaborative organizations.

The rest of this chapter is organized as follows. Section 6.2 describes the architecture and implementation of DRDoS attack alert system. Then, Section 6.3 explains the experiments and the operation results of the alert system. Section 6.4 discusses the system and the operation results, and Section 6.5 summarizes this chapter.

6.2 Alert System

In this section, we describe the architecture and implementation of DRDoS attack alert system using DRDoS honeypots. The basic idea of the alert system is to collect traffic data from DRDoS honeypots in real time, analyze the data, and send alerts of DRDoS attacks included in the data.

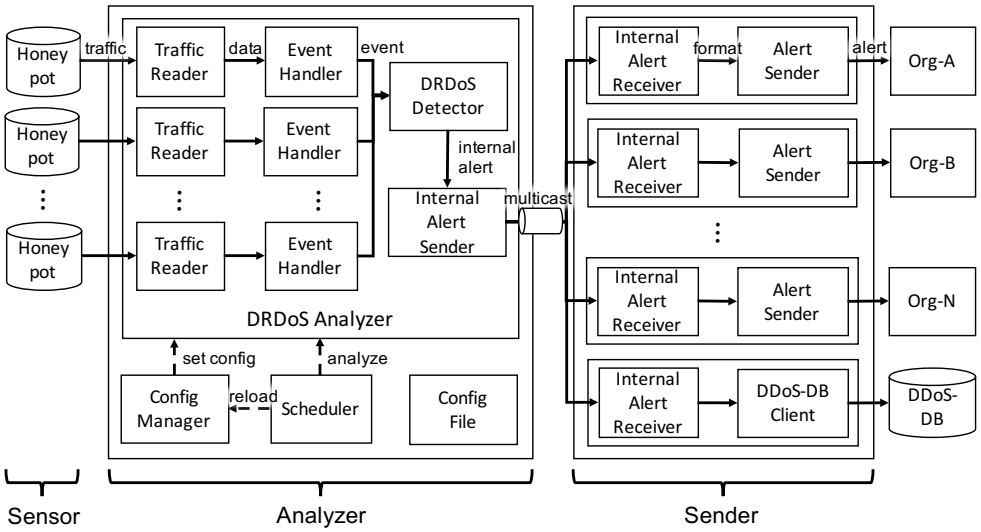


Figure 6.1: Architecture of DRDoS attack alert system.

For alerts to be helpful for network administrators, the alert system needs to be accurate and quick for real-time responses. Here, being "accurate" means that attack traffic which alerts indicates truly arrives at the victim, and being "quick" means that alerts are issued equal to or earlier than an existing detection engine. By building and operating an alert system that satisfies such requirements, we expect that the alert system enables network administrators to grasp the situation of attacks and take appropriate countermeasures in real time.

6.2.1 Architecture

Figure 6.1 shows the architecture of the alert system. The system consists of the three sections: "Sensor," "Analyzer," and "Sender."

Sensor

"Sensor" collects traffic data and transfers them to "Analyzer." DRDoS honeypots run at each observation point as described in Chapter 5, and collect the traffic data related to DRDoS attacks. The traffic data are transferred to the "Analyzer" periodically to analyze the data in real time.

Analyzer

The "Analyzer" analyzes the traffic data transferred from the "Sensor," and sends internal alerts to "Sender." More specifically, "Traffic Reader" reads the data from files, and "Event Handler" dissects and aggregates the data into "event" objects. An event object consists of the sequence of packets (see Section 5.3.1), and "DRDoS

Detector" examines the event objects. If the event is judged as an attack, then "Internal Alert Sender" sends the information of the event as an internal alert. "Scheduler" schedules these procedures and "Config Manager" manages the configurations. Here, the "Internal Alert Sender" sends internal alerts as multicast packets[1] so as to add/modify/remove senders of alerts easily in the "Sender".

Sender

The "Sender" sends alerts detected by the "Analyzer" to our collaborative organizations. When "Internal Alert Receivers" receive internal alerts from the "Analyzer," "Alert Senders" format the alert information depending on the destination organizations, and send the alert to the organizations respectively. "Alert Senders" can also filter alerts not related to the organizations. At the same time, the alerts are also stored into the database ("DDoS-DB") for the further research.

6.2.2 Alert Types

In the alert system, we provide two types of alerts to help network administrators comprehend the situation of DRDoS attacks.

Attack-Start Alert

An attack-start alert is issued when an attack starts. When the number of packets in an event has exceeded the threshold N_{attack} (see Section 5.3.1), the system sends this type of alert immediately. We provide this type of alert to help network administrators start mitigation of attacks as early as possible.

Attack-End Alert

An attack-end alert is issued when an attack ends. When no packets are seen in an event for more than T seconds, the system sends this type of alert. In the case of Figure 5.2, this type of alert is sent at the time of $t_{end} + T$. We provide this type of alert to help network administrators stop mitigation of attacks as early as possible.

Figure 6.2 shows an example of an alert message sent by the alert system, and Table 6.1 gives the list of the information included in alerts.

6.2.3 Implementation

The implementation of the alert system is as follows.

Sensor

The "Sensor" is a set of DRDoS honeypots. The implementation of the

[1] A technique to send packets to a group of interested receivers in a single transmission.

```
{
      "hostname": "[redacted].net",
      "elapsedtime": 3600,
      "as": "AS1[redacted]",
      "stoptime": "2015-10-31T08:09:49+09:00",
      "alerttime": "2015-10-31T08:11:37+09:00",
      "query": {
            "1x1.cz    ANY    IN": 59966
      },
      "maxpps": 23.35,
      "detecttime": "2015-10-31T07:09:59+09:00",
      "target": "[redacted].216.192",
      "service": "dns",
      "country": "Canada",
      "avepps": 16.38415300546448,
      "starttime": "2015-10-31T07:09:49+09:00",
      "sensorid": "sensor007",
      "totalpacket": 59966
}
```


Figure 6.2: Example of attack-end alert message in JSON format [93].

DRDoS honeypot is described in Section 5.2.2. Pcap files generated by the tcpdump utility [69] are the logs of the DRDoS honeypots, and the files are transferred to the "Analyzer" every minute by the scp command[2].

Analyzer

The "Analyzer" is implemented on an Ubuntu machine. Each component in the "Analyzer" is written in Python [94] language with the libraries of pcapy [95] and dpkt [96]. We used the GeoIP database provided by MaxMind [72] for geographical data such as countries and AS numbers of IP addresses.

Sender

The "Sender" is also implemented on an Ubuntu machine. Each component in the "Sender" is also written in Python language, and we support E-mail and fluentd [97] as methods to send alert information. To implement these methods, we use the Python's standard library for E-mail and fluent-logger-python [98] for a client library of the fluentd.

6.3 Experiments and Results

To verify the effectiveness of the alert system, we have been operating the system since February 2014 in the framework of a national research and

[2]A command to transfer files between two hosts securely based on the Secure Shell (SSH) protocol. SCP is short for "Secure CoPy."

Table 6.1: List of alert information.

(a) Attack-start alert.

Key	Value
alerttime	Time when the alert is issued.
as[1]	AS number and organization name of the target.
country[1]	Country of the target.
detecttime	Time when the number of packets exceeds the threshold N_{attack} (i.e. t_{thres})
query[2]	The number of queries per pair of (FQDN, type, class).
sensorid	Honeypot ID
service	Abused service (e.g. DNS, NTP, etc.).
starttime	Time when the attack starts (i.e. t_{start})
target	IP address of the target.
totalpacket	The number of packets observed by the honeypot.

(b) Attack-end alert.

Key	Value
(The same information as an attack-start alert.)	
elapsedtime	Duration of the attack [sec] (i.e. $t_{end} - t_{start}$)
stoptime	Time when the attack ends (i.e. t_{end})
maxpps	Maximum PPS value observed by the honeypot.
avepps	Average PPS value observed by the honeypot.
hostname	Hostname of the target by reverse lookup.

[1] We used the GeoIP Lite database [72] to identify the geolocation of the IP addresses.
[2] The "query" field is added when the attack is a DNS reflection attack.

development (R&D) project. As of November 2015, we provide DRDoS attack alerts to several ISPs in Japan.

In this section, we outline the operation of the alert system and show the results of the operation. Besides, as a result of the operation, we compare attack detection times between the alert system and an ISP's mass traffic detector.

6.3.1 Experiments

Table 6.2 summarizes the operation of the alert system in chronological order. We began providing attack-end alerts on February 27th, 2014, and began offering attack-start alerts on September 27, 2014. Initially, we used two DRDoS honeypots, but we added five DRDoS honeypots to provide more alerts. These honeypots work under ISP networks in Japan and support six protocols that can be abused for DRDoS attacks — QOTD, CHG, DNS, NTP,

Table 6.2: Operation of alert system.

Date	Operation
2014/02/27	Start providing attack-end alerts using two DRDoS honeypots with DNS and CHG services.
2014/05/10	Add two honeypots.
2015/05/17	Add three honeypots.
2014/09/27	Start providing attack-start alerts. Add supports of NTP and QOTD services.
2015/02/19	Add supports of SNMP and SSDP services.

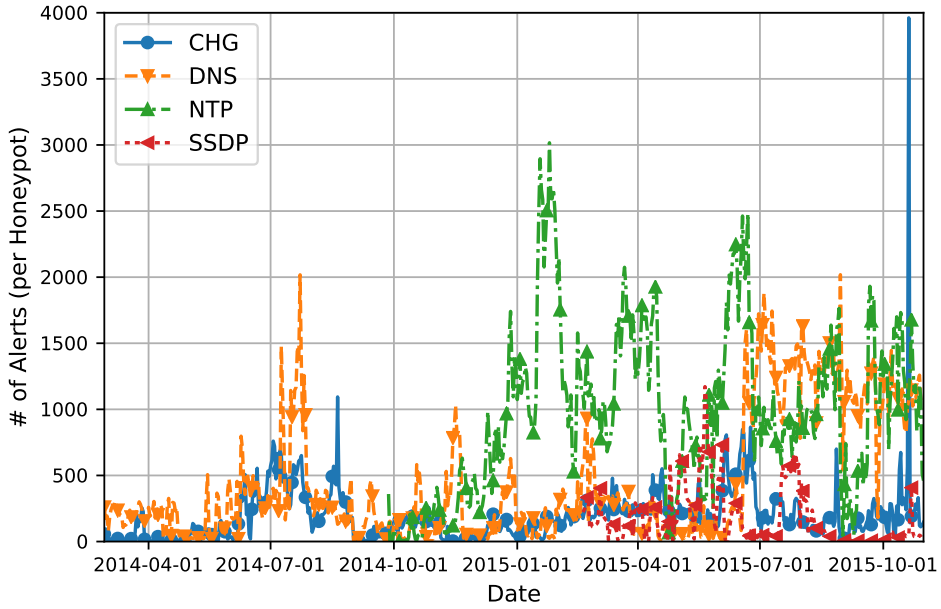


Figure 6.3: Number of DRDoS attack alerts (per honeypot).

SNMP, and SSDP — except one honeypot that supports only DNS.

For the thresholds of "events" (See Section 5.3.1) in the actual operation, we set N_{attack} to 100 in order to exclude scans, and we set T to 60 seconds so that we do not split events more than necessary and keep the quickness of alerts. We discuss the validity of these thresholds in Section 6.4.1, but we believe that these thresholds work well in the alert system from the results of the operation described later in this chapter.

Table 6.3: Number of DRDoS attack alerts in October 2015.

	QOTD	CHG	DNS	NTP	SNMP	SSDP
# of honeypots	6	6	7	6	6	6
# of alerts in total	460	65,373	241,267	224,928	159	9,935
# of alerts per honeypot	76	10,896	34,467	37,488	27	1,656
percentage	0.1%	12.9%	40.7%	44.3%	0.03%	2.0%

Table 6.4: Comparison of detection times between alert system and ISP's mass traffic detector.

DRDoS Honeypot	ISP's Detector	Difference [sec]
2014/10/■ 00:10:46	2014/10/■ 00:15:54	308
2014/11/■ 21:41:16	2014/11/■ 21:44:30	194
2014/11/■ 23:57:34	2014/11/■ 23:59:20	106
2014/11/■ 17:02:21	2014/11/■ 17:04:44	143

The parts of values in this table are masked for anonymity.

6.3.2 Results

Figure 6.3 shows the number of DRDoS attack alerts per honeypot, and Table 6.3 shows the overview of the results of DRDoS attack alerts in October 2015.

The alert system provided approximately 260 alerts in a day when we started providing. However, the number had increased since June 2014, and the system provided approximately 2,700 alerts to our collaborative organizations in a day in November 2015.

Here, we omit additional analyses of DRDoS attacks because we have shown the results in Chapter 5. In this chapter, we focus on the effectiveness of the alert system.

6.3.3 Comparison of Detection Times

The alert system observed 11 DRDoS attacks against ISP-A in Japan from October 9 to November 11, 2014. We investigated these attacks with the ISP and found that the four attacks were detected by the ISP's mass traffic detector. Table 6.4 shows the results of the comparison of the detection times between the alert system and the ISP's mass traffic detector.

The result shows that the alert system could detect these attacks earlier than ISP's detector, and the time difference is 188 seconds on average. By additional research, we confirm that the ISP observed some volume of the traffic related to the remaining seven attacks although the volume did not exceed the threshold the ISP defined.

6.4 Discussion

This section discusses the alert system and its operation results. First, Section 6.4.1 discusses the validity of the attack definition and the thresholds. Next, Section 6.4.2 discusses the delay of alerts in the system, and Section 6.4.3 describes the "accuracy" and "quickness". Lastly, Section 6.4.4 discusses the usefulness of the alert system.

6.4.1 Attack Definition and Thresholds

The alert system analyzes DRDoS attacks by the "event" defined in Section 5.3.1. An event is a sequence of packets which are grouped by the pair of honeypot ID, abused service, and source IP address, and if more than N_{attack} packets are observed without the gap of T seconds, then the event is judged as an attack. In this section, we discuss the validity of this definition and these thresholds.

In the event definition, we aggregate packets by the source IP address, but this definition stems from our experience. Many of DRDoS attacks that we have observed target a single IP address. However, we have also observed attacks that target some range of IP address space such as a /24 network (See Section 3.4.2). In that case, this definition does not work well to detect the whole of the attack. Therefore, we need to improve the definition to send more accurate alerts.

The thresholds we tentatively use in the current alert system ($N_{attack} = 100$ [packets] and $T = 60$ [seconds]) are also determined by our experience. If we set T to a smaller value, then the system can improve the quickness of alerts but it might split the attacks more than necessary. On the other hand, if we set T to a larger value, then the system can look over entire attacks but it loses the quickness of alerts. Therefore, in the current operation, we set T to 60 seconds (i.e. one minute) so that the alert system can observe the whole attack and does not lose the quickness. Similarly, if we set N_{attack} to a smaller value, the alert system can improve the quickness of alerts but scans can be included in alerts. On the other hand, if we set N_{attack} to a larger value, the system can exclude scans but it takes a longer time to reach the threshold. In the current operation, we set N_{attack} to 100 packets in order to exclude scans and keep the quickness.

Adjusting the definition and the thresholds is our future work, but the results of this chapter show sthat these tentative definition and thresholds work well to provide accurate and quick alerts to network administrators.

6.4.2 Alert Delay

The alert system transfers traffic data from the "Sensor" to the "Analyzer," analyzes the data in the "Analyzer," and sends alerts in the "Sender." That

is, these procedures result in the delay of alerts.

As described in Section 6.2, the alert system transfers pcap files every minute. Therefore, it takes about one minute to transfer the data from the "Sensor" to the "Analyzer." In addition, it takes extra one minute to analyze the data and exceed the threshold. Taking these delays into account, it takes about two minutes from the time when the attacks start/end to the time when the alerts are issued. We need to improve these latencies by optimizing the alert system. However, considering the result in Section 6.3.3, the current alert system is able to provide the alert information for real-time responses.

6.4.3 Accuracy and Quickness

As mentioned in Section 6.3.3, all the 11 attacks against the ISP-A observed by the alert system were also observed by the ISP-A. From this result, we can say that the alert system is accurate. Not all of the attacks observed by the DRDoS honeypots were detected as attacks by the ISP's detector, but the alert system can provide the useful information to the network administrators because some volume of the traffic truly reached the network.

Further, from the results of Table 6.4, we confirm that the alert system can detect attacks earlier than the ISP's mass traffic detector. We are not sure the reason, but we speculate that this is because the DRDoS honeypots observe only malicious traffic but the ISP's detector observes not only malicious traffic but also huge normal traffic and it takes a longer time to analyze the traffic. Because the number of the cases of the comparison is small, we need to perform more reliable analyses by continuing to provide alerts.

6.4.4 Usefulness

As discussed in this chapter, the alert system can provide accurate and quick alerts to network administrators for real-time responses. The way to utilize alert information effectively is a future challenge, but the administrators can prepare for mitigation as early as possible utilizing the information of attack-start alerts.

Besides, not only attack-start alerts but also attack-end alerts can provide the useful information. For example, if an attack is carried out and an administrator blocks the attack traffic on the router, it is necessary to recover quickly after the attack ends. In such a case, the attack-end alerts are useful as a trigger for objectively determining that the attack has ended. In addition, attack-end alerts are useful for sharing attack information as a database because the alerts include the various information shown in Table 6.1.

In this way, the alert system can provide useful information for real-time responses and information sharing, and therefore, the system can be expected as a system to support real-time responses against DRDoS attacks.

6.5 Summary

In this chapter, we propose DRDoS attack alert system using DRDoS honeypots as a countermeasure against DRDoS attacks. The alert system aims at helping network administrators to grasp the information of attacks quickly, and the administrators utilize this alert information for real-time responses such as the mitigation of attacks and the recovery from failure.

We have been operating this system and providing DRDoS attack alerts to several organizations under an R&D project in Japan. As a result of the operation, we compare attack detection times between the alert system and an ISP's mass traffic detector, and we confirm that the alert system is able to provide accurate and quick alerts for real-time responses.

Chapter 7

Conclusion and Future Work

7.1 Conclusion

DDoS attacks have become a significant threat on the Internet, and extensive researches have been made to work on this threat. In particular, DRDoS attacks have become popular as a method to launch DDoS attacks since 2013, and there is a compelling need to take effective countermeasures. However, the inside of DRDoS attacks are not well studied or reported, and therefore, we decided to observe DRDoS attacks in the wild and analyze the trends and characteristics for countermeasures.

In this dissertation, we have proposed observation systems of DRDoS attacks and countermeasures against them. In Chapter 3, we have proposed an observation system called DNS honeypot. DNS honeypot is a decoy DNS cache server that works as an open resolver on the Internet, and it gives us special insight into DNS reflection attacks. As a result of the experiment, we have confirmed that DNS honeypot can observe DNS reflection attacks and the number of attacks had increased since 2013. In Chapter 4, we have analyzed the correlation of DNS queries that DNS honeypots and a darknet sensor observe. As a result of analysis, we have discovered that some attackers conduct scans using the same domain names as DNS reflection attacks before they launch attacks. This knowledge will lead to proactive countermeasures against DNS reflection attacks such as the blacklisting of domain names before attacks. In Chapter 5, we have improved DNS honeypot to DRDoS honeypot in order to observe not only DNS reflection attacks but also other types of DRDoS attacks. As a result of the experiment, we have revealed the facts that the DRDoS honeypots observed four thousand DRDoS attacks in a day, half of the attacks lasted only for less than five minutes, 90% of the victims aggregated by the IP address were attacked only once for half a year, and 33% of the attacks, on the contrary, went to only ten ASes. In Chapter 6, we have proposed DRDoS alert system using DRDoS honeypots for real-time responses against DRDoS attacks. We

have been operating this system and providing DRDoS attack alerts to several organizations under an R&D project in Japan. As a result of the operation, we have confirmed that the system is able to provide accurate and quick alerts for real-time responses.

Our research we have described in this dissertation do not provide a perfect solution to overcome the threat of DRDoS attacks, but we believe our research will lead to effective countermeasures against DRDoS attacks.

7.2 Future Work

Many studies have been published to tackle the threats of DRDoS attacks. However, unfortunately, the threat remains severe as of November 2016, and we will continue to devote ourselves to the study of DRDoS attacks.

As future work, we will continue to develop DRDoS honeypot so as to observe more DRDoS attacks. In addition, we would like to improve DRDoS attack alert system so that it can provide more accurate and quick alerts for real-time responses. Furthermore, we will not only provide DRDoS attack alerts but also publish periodical reports of DRDoS attacks in the future.

And finally, we mainly discuss DRDoS attacks in this dissertation, but we will try to observe other types of DDoS attacks to make effective countermeasures against DDoS attacks that threaten our daily lives on the Internet.

Bibliography

[1] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, Apr. 2004. [Online]. Available: http://doi.acm.org/10.1145/997150.997156

[2] C. Douligeris and A. Mitrokotsa, "DDoS Attacks and Defense Mechanisms: Classification and State-of-the-art," *Computer Networks*, vol. 44, no. 5, pp. 643–666, Apr. 2004. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2003.10.003

[3] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Communications Surveys Tutorials*, vol. 15, no. 4, pp. 2046–2069, Fourth 2013.

[4] Akamai Technologies. (2014) DD4BC: PLXsert warns of Bitcoin extortion attempts. [Online]. Available: https://blogs.akamai.com/2014/12/dd4bc-anatomy-of-a-bitcoin-extortion-campaign.html

[5] Akamai Technologies. (2015) Operation Profile: Armada Collective. [Online]. Available: https://blogs.akamai.com/2015/11/operation-profile-armada-collective.html

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[7] AusCERT. (1999) Domain Name System (DNS) Denial of Service (DoS) Attacks. [Online]. Available: https://www.auscert.org.au/render.html?it=80

[8] The Spamhaus Project Ltd., http://www.spamhaus.org/.

[9] Cloudflare, Inc., http://www.cloudflare.com/.

[10] Cloudflare, Inc. (2013) The DDoS That Almost Broke the Internet. [Online]. Available: https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/

[11] OVH, https://www.ovh.com/.

[12] Cloudflare, Inc. (2014) Technical Details Behind a 400Gbps NTP Amplification DDoS Attack. [Online]. Available: http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/

[13] J. J. Santanna and A. Sperotto, "Characterizing and mitigating the ddos-as-a-service phenomenon," in *Monitoring and securing virtualized networks and services*, ser. Lecture notes in computer science, A. Sperotto, G. Doyen, S. Latré, M. Charalambides, and B. Stiller, Eds., vol. 8508. Berlin, Germany: Springer, June 2014, pp. 74–78. [Online]. Available: http://doc.utwente.nl/93590/

[14] J. J. Santanna, R. van Rijswijk-Deij, A. Sperotto, M. Wierbosch, L. Zambenedetti Granville, and A. Pras, "Booters - an analysis of DDoS-as-a-Service attacks," in *IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, R. Badonnel, J. Xiao, S. Ata, F. De Turck, V. Groza, and C. R. P. dos Santos, Eds. Piscataway, NJ, USA: IEEE Computer Society, May 2015, pp. 243–251. [Online]. Available: http://doc.utwente.nl/96839/

[15] J. J. Santanna, R. Durban, A. Sperotto, and A. Pras, "Inside Booters: an analysis on operational databases," in *IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, R. Badonnel, J. Xiao, S. Ata, F. De Turck, V. Groza, and C. R. P. dos Santos, Eds. Piscataway, NJ, USA: IEEE Computer Society, May 2015, pp. 432–440. [Online]. Available: http://doc.utwente.nl/96840/

[16] M. Karami, Y. Park, and D. McCoy, "Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services," in *Proceedings of the 25th International Conference on World Wide Web*, ser. WWW '16. Republic and Canton of Geneva, Switzerland: International World Wide Web Conferences Steering Committee, 2016, pp. 1033–1043. [Online]. Available: https://doi.org/10.1145/2872427.2883004

[17] L. T. Heberlein and M. Bishop, "Attack Class: Address Spoofing," in *Proceedings of the 19th National Information Systems Security Conference*, 1996, pp. 371–377.

[18] D. S. P. Ferguson. (2000) RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. [Online]. Available: http://www.ietf.org/rfc/rfc2827.txt

[19] K. Park and H. Lee, "On the Effectiveness of Route-based Packet Filtering for Distributed DoS Attack Prevention in Power-law Internets," *SIGCOMM Comput. Commun. Rev.*, vol. 31, no. 4, pp. 15–26, Aug. 2001. [Online]. Available: http://doi.acm.org/10.1145/964723.383061

[20] R. Beverly and S. Bauer, "The Spoofer Project: Inferring the Extent of Source Address Filtering on the Internet," in *Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop*, ser. SRUTI'05. Berkeley, CA, USA: USENIX Association, 2005, pp. 8–8. [Online]. Available: http://dl.acm.org/citation.cfm?id=1251282.1251290

[21] T. Ehrenkranz and J. Li, "On the State of IP Spoofing Defense," *ACM Trans. Internet Technol.*, vol. 9, no. 2, pp. 6:1–6:29, May 2009. [Online]. Available: http://doi.acm.org/10.1145/1516539.1516541

[22] Spoofer Project, https://www.caida.org/projects/spoofer/.

[23] R. Shankesi, M. AlTurki, R. Sasse, C. A. Gunter, and J. Meseguer, "Model-checking DoS Amplification for VoIP Session Initiation," in *Proceedings of the 14th European Conference on Research in Computer Security*, ser. ESORICS'09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 390–405. [Online]. Available: http://dl.acm.org/citation.cfm?id=1813084.1813116

[24] M. Kührer, T. Hupperich, C. Rossow, and T. Holz, "Exit from Hell? Reducing the Impact of Amplification DDoS Attacks," in *Proceedings of the 23rd USENIX Conference on Security Symposium*, ser. SEC'14. Berkeley, CA, USA: USENIX Association, 2014, pp. 111–125. [Online]. Available: http://dl.acm.org/citation.cfm?id=2671225.2671233

[25] C. Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse," in *Proceedings of the 2014 Network and Distributed System Security Symposium, NDSS*, 2014.

[26] Open Resolver Scanning Project, https://dnsscan.shadowserver.org/.

[27] Open Resolver Project, http://www.openresolverproject.org/.

[28] Open NTP Project, http://openntpproject.org/.

[29] H. Tsunoda, Y. Nemoto, K. Ohta, and A. Yamamoto, "A simple response packet confirmation method for DRDoS detection," in *2006 8th International Conference Advanced Communication Technology*, vol. 3, Feb 2006, pp. 5–1561.

[30] G. Kambourakis, T. Moschos, D. Geneiatakis, and S. Gritzalis, "A Fair Solution to DNS Amplification Attacks," in *Proceedings of the Second International Workshop on Digital Forensics and Incident Analysis*, ser. WDFIA '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 38–47. [Online]. Available: http://dx.doi.org/10.1109/WDFIA.2007.2

[31] G. Kambourakis, T. Moschos, D. Geneiatakis, and S. Gritzalis, "Detecting DNS Amplification Attacks," in *Proceedings of the Second International Conference on Critical Information Infrastructures Security*, ser. CRITIS'07. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 185–196. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-89173-4_16

[32] H. Tsunoda, K. Ohta, A. Yamamoto, N. Ansari, Y. Waizumi, and Y. Nemoto, "Detecting DRDoS Attacks by a Simple Response Packet Confirmation Mechanism," *Computer Communications*, vol. 31, no. 14, pp. 3299–3306, Sep. 2008. [Online]. Available: http://dx.doi.org/10.1016/j.comcom.2008.05.033

[33] W. Wei, F. Chen, Y. Xia, and G. Jin, "A Rank Correlation Based Detection against Distributed Reflection DoS Attacks," *IEEE Communications Letters*, vol. 17, no. 1, pp. 173–175, January 2013.

[34] P. M. Priya, V. Akilandeswari, S. M. Shalinie, V. Lavanya, and M. S. Priya, "The Protocol Independent Detection and Classification (PIDC) system for DRDoS attack," in *2014 International Conference on Recent Trends in Information Technology*, April 2014, pp. 1–7.

[35] M. Backes, T. Holz, C. Rossow, T. Rytilahti, M. Simeonovski, and B. Stock, "On the Feasibility of TTL-Based Filtering for DRDoS Mitigation," in *Research in Attacks, Intrusions, and Defenses: 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings*, F. Monrose, M. Dacier, G. Blanc, and J. Garcia-Alfaro, Eds. Cham: Springer International Publishing, 2016, pp. 303–322. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-45719-2_14

[36] C. Dietzel, A. Feldmann, and T. King, "Blackholing at ixps: On the effectiveness of ddos mitigation in the wild," in *Passive and Active Measurement - 17th International Conference, PAM 2016, Heraklion, Greece, March 31 - April 1, 2016. Proceedings*, 2016, pp. 319–332. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-30505-9_24

[37] Akamai Technologies. (2016) Threat Advisory: #OpKillingBay Expands Targets Across Japan. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/opkillingbay-expands-targets-across-japan-threat-advisory.pdf

[38] L.-C. Chen, T. A. Longstaff, and K. M. Carley, "Characterization of defense mechanisms against distributed denial of service attacks," *Computers & Security*, vol. 23, no. 8, pp. 665 – 678, 2004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404804001774

[39] Peng, Tao and Leckie, Christopher and Ramamohanarao, Kotagiri, "Survey of network-based defense mechanisms countering the dos and ddos problems," *ACM Comput. Surv.*, vol. 39, no. 1, Apr. 2007. [Online]. Available: http://doi.acm.org/10.1145/1216370.1216373

[40] U. Tariq, M. Hong, and K.-s. Lhee, "A Comprehensive Categorization of DDoS Attack and DDoS Defense Techniques," in *Advanced Data Mining and Applications: Second International Conference, ADMA 2006, Xi'an, China, August 14-16, 2006 Proceedings*, X. Li, O. R. Zaïane, and Z. Li, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 1025–1036. [Online]. Available: http://dx.doi.org/10.1007/11811305_112

[41] S. M. Specht and R. B. Lee, "Distributed denial of service: Taxonomies of attacks, tools, and countermeasures," in *Proceedings of the ISCA 17th International Conference on Parallel and Distributed Computing Systems, September 15-17, 2004, The Canterbury Hotel, San Francisco, California, USA*, 2004, pp. 543–550.

[42] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang, "Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures," in *Proceedings of the 2009 Fourth International Conference on Innovative Computing, Information and Control*, ser. ICICIC '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 1184–1187. [Online]. Available: http://dx.doi.org/10.1109/ICICIC.2009.127

[43] E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah, and R. Alfaris, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," *CoRR*, vol. abs/1208.0403, 2012. [Online]. Available: http://arxiv.org/abs/1208.0403

[44] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," in *Proceedings of the 9th USENIX Conference on Offensive Technologies*, ser. WOOT'15. Berkeley, CA, USA: USENIX Association, 2015, pp. 9–9. [Online]. Available: http://dl.acm.org/citation.cfm?id=2831211.2831220

[45] Krebs on Security, https://krebsonsecurity.com/.

[46] Krebs on Security. (2016) Source Code for IoT Botnet 'Mirai' Released. [Online]. Available: https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

[47] Krebs on Security. (2016) KrebsOnSecurity Hit With Record DDoS. [Online]. Available: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[48] J. Postel *et al.* (1981) RFC 791: Internet protocol. [Online]. Available: http://www.ietf.org/rfc/rfc791.txt

[49] B. Sieklik, R. Macfarlane, and W. J. Buchanan, "Evaluation of TFTP DDoS amplification attack," *Computers & Security*, vol. 57, pp. 67 – 92, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404815001285

[50] Akamai Technologies. (2016) New DDoS Reflection/Amplification Method Exploits TFTP. [Online]. Available: https://blogs.akamai.com/2016/06/new-ddos-reflectionamplification-method-exploits-tftp.html

[51] Akamai Technologies. (2015) Threat Advisory: NetBIOS name server, RPC portmap and Sentinel reflection DDoS. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/ddos-reflection-netbios-name-server-rpc-portmap-sentinel-udp-threat-advisory.pdf

[52] Corero Network Security, Inc. (2016) Corero Team Discovers a New DDoS Vector. [Online]. Available: https://www.corero.com/blog/770-corero-team-discovers-a-new-ddos-vector.html

[53] Akamai Technologies. (2015) Threat Advisory: RIPv1 Reflection DDoS. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/ripv1-reflection-ddos-threat-advisory.pdf

[54] Default Deny. (2015) MC-SQLR Amplification: MS SQL Server Resolution Service enables reflected DDoS with 440x amplification. [Online]. Available: http://kurtaubuchon.blogspot.com/2015/01/mc-sqlr-amplification-ms-sql-server.html

[55] Akamai Technologies. (2015) SECURITY BULLETIN: MS SQL REFLECTION DDOS. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/ms-sql-server-reflection-ddos-mc-sqlr-threat-advisory.pdf

[56] Akamai Technologies. (2016) Threat Advisory: mDNS Reflection DDoS. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-mdns-reflection-ddos-threat-advisory.pdf

[57] M. Kührer, T. Hupperich, C. Rossow, and T. Holz, "Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks," in *Proceedings of the 8th USENIX Conference on Offensive Technologies*, ser. WOOT'14. Berkeley, CA, USA: USENIX Association, 2014, pp. 4–4. [Online]. Available: http://dl.acm.org/citation.cfm?id=2671293.2671297

[58] F. J. Ryba, M. Orlinski, M. Wählisch, C. Rossow, and T. C. Schmidt, "Amplification and DRDoS Attack Defense - A Survey and New

Perspectives," *CoRR*, vol. abs/1505.07892, 2015. [Online]. Available: http://arxiv.org/abs/1505.07892

[59] S. M. Bellovin, "Security Problems in the TCP/IP Protocol Suite," *SIGCOMM Comput. Commun. Rev.*, vol. 19, no. 2, pp. 32–48, Apr. 1989. [Online]. Available: http://doi.acm.org/10.1145/378444.378449

[60] Cloudflare, Inc. (2015) Deprecating the DNS ANY meta-query type. [Online]. Available: https://blog.cloudflare.com/deprecating-dns-any-meta-query-type/

[61] The Measurement Factory, http://www.measurement-factory.com/.

[62] T. Peng, C. Leckie, and K. Ramamohanarao, "Protection from distributed denial of service attacks using history-based IP filtering," in *Communications, 2003. ICC '03. IEEE International Conference on*, vol. 1, May 2003, pp. 482–486 vol.1.

[63] P. Mockapetris. (1987) RFC1034: Domain names: concepts and facilities. [Online]. Available: http://www.ietf.org/rfc/rfc1034.txt

[64] P. Mockapetris. (1987) RFC1035: Domain name: implementation and specification. [Online]. Available: http://www.ietf.org/rfc/rfc1035.txt

[65] Prolexic Technologies, Inc., http://www.prolexic.com/.

[66] Ubuntu, http://ubuntu.com/.

[67] BIND, https://www.isc.org/downloads/bind/.

[68] iptables, http://www.netfilter.org/projects/iptables/index.html.

[69] tcpdump, http://www.tcpdump.org/.

[70] WireShark. (2015) Development/LibpcapFileFormat. [Online]. Available: https://wiki.wireshark.org/Development/LibpcapFileFormat

[71] P. Vixie. (1999) RFC2671: Extension Mechanisms for DNS (EDNS0). [Online]. Available: http://www.ietf.org/rfc/rfc2671.txt

[72] MaxMind, Inc., https://www.maxmind.com/.

[73] Alexa Internet, Inc., http://www.alexa.com/.

[74] M. West and S. McCann. (2006) RFC4413: TCP/IP Field Behavior. [Online]. Available: http://www.ietf.org/rfc/rfc4413.txt

[75] D. Atkins and R. Austein. (2004) RFC3833: Threat Analysis of the Domain Name System. [Online]. Available: http://www.ietf.org/rfc/rfc3833.txt

[76] A. Hubert and R. van Mook. (2009) RFC 5452: Measures for making DNS more resilient against forged answers. [Online]. Available: http://www.ietf.org/rfc/rfc5452.txt

[77] NICTER, http://www.nicter.jp/.

[78] T. Takehisa, D. Inoue, M. Eto, K. Yoshioka, T. Kasama, J. Nakazato, and K. Nakao, "NONSTOP: Secure remote analysis platform for cybersecurity information," *Technical Report of IEICE. Information and Communication System Security*, vol. 113, no. 95, pp. 85–90, 2013.

[79] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson, "The Internet Motion Sensor: A Distributed Blackhole Monitoring System," in *Proceedings of Network and Distributed System Security Symposium (NDSS '05)*, 2005, pp. 167–179.

[80] D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, and K. Nakao, "nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis," in *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing*, April 2008, pp. 58–66.

[81] Z. Durumeric, M. Bailey, and J. A. Halderman, "An Internet-wide View of Internet-wide Scanning," in *Proceedings of the 23rd USENIX Conference on Security Symposium*, ser. SEC'14. Berkeley, CA, USA: USENIX Association, 2014, pp. 65–78.

[82] C. Fachkha and M. Debbabi, "Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1197–1227, Secondquarter 2016.

[83] Internet Systems Consortium, https://www.isc.org/.

[84] RIPE Network Coordination Centre, https://www.ripe.net/.

[85] L. Bilge, S. Sen, D. Balzarotti, E. Kirda, and C. Kruegel, "Exposure: A Passive DNS Analysis Service to Detect and Report Malicious Domains," *ACM Trans. Inf. Syst. Secur.*, vol. 16, no. 4, pp. 14:1–14:28, Apr. 2014. [Online]. Available: http://doi.acm.org/10.1145/2584679

[86] Google Public DNS, https://developers.google.com/speed/public-dns/.

[87] quoted, http://www.mrp3.com/webutil/quoted.html.

[88] xinetd, http://www.xinetd.org/.

[89] Unbound, https://www.unbound.net/.

[90] NTP Project, http://www.ntp.org/.

[91] Net-SNMP, http://www.net-snmp.org/.

[92] The Measurement Factory: IPv4 Heatmaps, http://maps.measurement-factory.com/.

[93] JavaScript Object Notation (JSON), http://www.json.org/index.html.

[94] Python, https://www.python.org/.

[95] pcapy, https://github.com/CoreSecurity/pcapy.

[96] dpkt, https://github.com/kbandla/dpkt.

[97] Fluentd, http://www.fluentd.org/.

[98] A Python structured logger for Fluentd, https://github.com/fluent/fluent-logger-python.

List of Publications

Reviewed Papers in Journals

1. Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto: Observing DNS Amplification Attacks with DNS Honeypot, Journal of Information Processing, Vol.55, No.9, pp.2021-2033, 2014. *(in Japanese)*

   牧田大佑，吉岡克成，松本勉：DNS ハニーポットによる DNS アンプ攻撃の観測，情報処理学会論文誌，Vol.55，No.9，pp.2021-2033，2014.

2. Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto: Correlation Analysis between DNS Honeypot and Darknet toward Proactive Countermeasures against DNS Amplification Attacks, Journal of Information Processing, Vol.56, No.3, pp.921-931, 2015. *(in Japanese)* **[JIP/Specially Selected Paper]**

   牧田大佑，吉岡克成，松本勉，中里純二，島村隼平，井上大介：DNS アンプ攻撃の事前対策へ向けた DNS ハニーポットとダークネットの相関分析，情報処理学会論文誌，Vol.56，No.3，pp.921-931，2015.（情報処理学会論文誌 ジャーナル/JIP 特選論文）

3. Daisuke Makita, Tomomi Nishizoe, Katsunari Yoshioka, Tsutomu Matsumoto, Daisuke Inoue, Koji Nakao: DRDoS Attack Alert System for Early Incident Response, Journal of Information Processing, Vol.57, No.9, pp.1974-1985, 2016. *(in Japanese)* **[JIP/Specially Selected Paper]**

   牧田大佑，西添友美，吉岡克成，松本勉，井上大介，中尾康二：早期インシデント対応を目的とした DRDoS 攻撃アラートシステム，情報処理学会論文誌，Vol.57，No.9，pp.1974-1985，2016.（情報処理学会論文誌 ジャーナル/JIP 特選論文）

Reviewed Papers in International Conference Proceedings

1. Lukas Krämer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, Christian Rossow: AmpPot:

Monitoring and Defending Amplification DDoS Attacks, in Proceedings of the 18th International Symposium on Research in Attacks, Intrusions and Defenses (RAID15).

2. Arman Noroozian, Maciej Korczyński, Carlos Hernandez Gañan, Daisuke Makita, Katsunari Yoshioka, Michel van Eeten: Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service, in Proceedings of the 19th International Symposium on Research in Attacks, Intrusions and Defenses (RAID16).

Technical Reports

1. Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto: Observing Malicious Activities with DNS Honeypot, Information Processing Society of Japan (IPSJ), IPSJ SIG Technical Report on Computer Security (CSEC), 2013-CSEC-62, 2013. *(in Japanese)*

   牧田大佑，吉岡克成，松本勉：DNS ハニーポットによる不正活動観測，情報処理学会，研究報告コンピュータセキュリティ（CSEC），2013-CSEC-62，2013.

2. Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto, Junji Nakazato, Jumpei Shimamura, Daisuke Inoue: Correlation Analysis between DNS Honeypot and Darknet for Proactive Countermeasures of DNS Amplification Attacks, The Institute of Electronics, Information and Communication Engineers (IEICE), Symposium on Cryptography and Information Security (SCIS), 2014. *(in Japanese)*

   牧田大佑，吉岡克成，松本勉，中里純二，島村隼平，井上大介：DNS アンプ攻撃の早期対策を目的とした DNS ハニーポットとダークネットの突合分析，電子情報通信学会，暗号と情報セキュリティシンポジウム（SCIS），2014.

3. Jumpei Urakawa, Ayumu Kubota, Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto: A Study of Early Detection and Scale Estimation of DNS Amplification Attack, The Institute of Electronics, Information and Communication Engineers (IEICE), The IEICE General Conference, 2014. *(in Japanese)*

   浦川順平，窪田歩，牧田大祐，吉岡克成，松本勉：DNS アンプ攻撃の早期検知と規模推定に関する一考察，電子情報通信学会，総合大会講演論文集，2014.

4. Takuya Tsutsumi, Yoshiaki Nonogaki, Rui Tanabe, Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto: Observing Distributed Reflection Denial-of-Service Attacks by Several Kinds of Honeypots. Information Processing Society of Japan (IPSJ), IPSJ SIG Technical

Report on Computer Security (CSEC), 2014-CSEC-65, 2014. *(in Japanese)*

筒見拓也，野々垣嘉晃，田辺瑠偉，牧田大佑，吉岡克成，松本勉：複数種類のハニーポットによる DRDoS 攻撃の観測，情報処理学会，研究報告コンピュータセキュリティ（CSEC），2014-CSEC-65，2014.

5. Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto, Jumpei Shimamura, Daisuke Inoue, Koji Nakao: Observing DNS Water Torture by DNS Honeypot Information Processing Society of Japan (IPSJ), Computer Security Symposium (CSS), 2014. *(in Japanese)*

   牧田大佑，吉岡克成，松本勉，島村隼平，井上大介，中尾康二：DNS ハニーポットによる DNS Water Torture の観測，情報処理学会，コンピュータセキュリティシンポジウム（CSS），2014.

6. Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Takuya Tsutsumi, Fumihiro Kanei, Hiroshi Mori, Katsunari Yoshioka, Tsutomu Matsumoto, Daisuke Inoue, Koji Nakao: Development of Integrated DRDoS Attack Observation System toward Early Response, The Institute of Electronics, Information and Communication Engineers (IEICE), Symposium on Cryptography and Information Security (SCIS) , 2015. *(in Japanese)*

   牧田大佑，西添友美，小出駿，筒見拓也，金井文宏，森博志，吉岡克成，松本勉，井上大介，中尾康二：早期対応を目的とした統合型 DRDoS 攻撃観測システムの構築，電子情報通信学会，暗号と情報セキュリティシンポジウム（SCIS），2015.

7. Tomomi Nishizoe, Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto: Observing DRDoS Attacks with Protocol-noncompliant Honeypot, The Institute of Electronics, Information and Communication Engineers (IEICE), Symposium on Cryptography and Information Security (SCIS), 2015. *(in Japanese)*

   西添友美，牧田大佑，吉岡克成，松本勉：プロトコル非準拠のハニーポットによる DRDoS 攻撃の観測，電子情報通信学会，暗号と情報セキュリティシンポジウム（SCIS），2015.

8. Jumpei Urakawa, Yukiko Sawaya, Akira Yamada, Ayumu Kubota, Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto: An Early Scale Estimation of DRDoS Attack Monitoring Honeypot, The Institute of Electronics, Information and Communication Engineers (IEICE), Symposium on Cryptography and Information Security (SCIS), 2015. *(in Japanese)*

   浦川順平，澤谷雪子，山田明，窪田歩，牧田大佑，吉岡克成，松本勉：ハ

ニーポット監視による DRDoS 攻撃の早期規模推定，電子情報通信学会，暗号と情報セキュリティシンポジウム（SCIS），2015.

9. Daisuke Makita, Tomomi Nishizoe, Katsunari Yoshioka, Tsutomu Matsumoto, Daisuke Inoue, Koji Nakao: An Analysis of Attack Targets Observed by DRDoS Honeypots, Information Processing Society of Japan (IPSJ), Computer Security Symposium (CSS), 2015. *(in Japanese)*

   牧田大佑，西添友美，吉岡克成，松本勉，井上大介，中尾康二：DRDoS ハニーポットが観測した攻撃の履歴を用いた攻撃対象の傾向分析，情報処理学会，コンピュータセキュリティシンポジウム（CSS），2015.

10. Takashi Koide, Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto: Observation and Analysis of TCP-based Reflection Attacks Using Honeypot, Information Processing Society of Japan (IPSJ), Computer Security Symposium (CSS), 2015. *(in Japanese)*

    小出駿，牧田大佑，吉岡克成，松本勉：ハニーポットによる TCP リフレクション攻撃の観測と分析，情報処理学会，コンピュータセキュリティシンポジウム（CSS），2015.

11. Jumpei Urakawa, Akira Yamada, Ayumu Kubota, Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto: Evaluation of Cyber Attack Prediction using Honeypot Sensors for ISP, The Institute of Electronics, Information and Communication Engineers (IEICE), The IEICE General Conference, 2016. *(in Japanese)*

    浦川順平，山田明，窪田歩，牧田大祐，吉岡克成， 松本勉：ISP 運用におけるハニーポットセンサ観測データを用いたサイバー攻撃予測の評価，電子情報通信学会，2016 年電子情報通信学会総合大会，企画公演セッション，国際連携によるサイバー攻撃の予知・即応，2016.

12. Katsunari Yoshioka, Daisuke Makita, Tomomi Nishizoe, Tsutomu Matsumoto, Daisuke Inoue, Koji Nakao: Real-Time Detection and Alerting of DRDoS Attacks, The Institute of Electronics, Information and Communication Engineers (IEICE), The IEICE General Conference, 2016. *(in Japanese)*

    吉岡克成，牧田大佑，西添友美，松本勉，井上大介，中尾康二：DRDoS 攻撃のリアルタイム検知と即時警報システム，電子情報通信学会，2016 年電子情報通信学会総合大会，企画公演セッション，国際連携によるサイバー攻撃の予知・即応，2016.

13. Takemasa Kamatani, Ayumu Senga, Kosuke Murakami, Daisuke Makita, Katsunari Yoshioka, Koji Nakao: Quick response activity against DRDoS attacks utilizing AmpPot Information Processing Society of Japan (IPSJ), Computer Security Symposium

(CSS), 2016. *(in Japanese)*

蒲谷武正，千賀渉，村上洸介，牧田大佑，吉岡克成，中尾康二：AmpPot を活用した DRDoS 攻撃対応早期化の取り組み，情報処理学会，コンピュータセキュリティシンポジウム（CSS），2016.

14. Tomomi Nishizoe, Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto: Analysis of DRDoS attacks Evading CDN by DRDoS Honeypots, Information Processing Society of Japan (IPSJ), Computer Security Symposium (CSS), 2016. *(in Japanese. The title was translated tentatively.)*

    西添友美，牧田大佑，吉岡克成，松本勉：DRDoS ハニーポットが観測した CDN を回避する攻撃の分析，情報処理学会，コンピュータセキュリティシンポジウム（CSS），2016.

Invited Talk

1. Daisuke Makita: Correlation Analysis Between DNS Honeypot and Darknet for Proactive Countermeasures of DNS Amplification Attacks, Invited Talk in International Workshop on Security (IWSEC), 2014.

Poster in International Conference

1. Takashi Koide, Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto: Observation and Analysis of TCP-based Reflection DDoS Attacks Using Honeypot, Posters of the 18th International Symposium on Research in Attacks, Intrusions and Defenses (RAID15).