5-3 Development of Honeypot to Observe DRDoS Attacks

Daisuke MAKITA and Katsunari YOSHIOKA

We have been developing a honeypot system called AmpPot which observes DRDoS attacks. In this paper, we describe the overview of AmpPot and show the trend and characteristics of DRDoS attacks observed by AmpPot. In addition, we explain an alerting system using observation results of AmpPot as a countermeasure against DRDoS attacks.

1 Introduction

As services on the Internet became widely accepted and available, cyber-attacks attempting to deny such services (Denial-of-Service Attack: DoS Attack) have emerged as serious threats on the Internet. DDoS attacks are executed in various ways, and they are generally separated into two types; the attacks of the first type are accomplished by taking advantage of vulnerabilities existing in the service-providing programs; those of the second type transmit a vast number of communication or service-request messages at a time to impose excessive loads on the service systems. Protection against attacks of the second type is particularly difficult because they are often executed in a distributed way by using bots[*1] that attackers prepare in advance (Distributed Denial-of-Service Attack: DDoS Attack). DDoS attacks have been executed in various ways; for example, a vast number of TCP-SYN packets (SYN-FLOOD attack) or UDP packets (UDP-FLOOD attack) are sent to the targets. Recently, in addition to those types of attacks, attacks called Distributed Reflection Denial-of-Service (DRDoS Attack) have emerged as a more serious threat.

In a DRDoS attack, the attacker sends a vast number of packets to its target by “reflecting” the attacker-created communications on the machines existing on the Internet; the attacker forges a fake request packet which has, at its sender address, the IP address of the target, and sends the fake packets to a vast number of machines on the Internet to make the response packets go to the target. As a consequence, the target is forced to consume its resources too much to provide its regular services. DRDoS attacks, of which the existence was already known in around 2000, have become a mainstream means of DDoS attack, having been used widely since they were used in an attack on Spamhaus[*2] in March 2013 [1]—for example, some hacker groups use DRDoS attacks as a means of DDoS attack, including Anonymous[*3], which has frequently been covered by the media and DD4BC [2], which demands ransoms by blackmailing targets using DDoS attacks.

Furthermore, recently, DDoS attack providing services[*4] called Booter or Stresser have reportedly emerged [3][4], enabling ordinary users without knowledge of cyber-attacks to easily execute DDoS attacks.

For the purpose of investigating actual DRDoS attacks and establishing countermeasures, we have been putting efforts into research and development of a “honeypot” which is used for making observations for DRDoS attacks (hereinafter, our honeypot is referred to as AmpPot[5][6]). In this article, we will introduce AmpPot and our analyses of the attacks we observed, and then present our findings on the trends in and the characteristics of DRDoS attacks. Then, we will introduce a DRDoS Alert System, which we have developed and been operating.

The rest of this article is organized as follows. In Section **2**, we will describe our research and development background and the characteristics of DRDoS attacks. Then, in Section **3**, we will introduce the configuration of

[*1] A type of malicious software (malware) that works following attacker’s instructions

[*2] A non-profit organization which provides information on cyber-attack countermeasures, focusing on spam-mail measures (https://www.spamhaus.org/)

[*3] An international organization which engages in protest activities under the name of “Anonymous”; some members have executed cyber-attacks using various means including DDoS attacks.

[*4] Officially, Booter / Stresser provides load-test services; however, actually, their services have been used for DDoS attacks.

AmpPot which we have been developing, our experiments on AmpPot, and how we have been operating AmpPot. In Section **4**, we will introduce our analyses of the DRDoS attacks we have observed using AmpPots. Then, in Section **5**, we will introduce the DRDoS Attack Alert System which employs AmpPots. Finally, in Section **6**, we will conclude the article, and in addition mention our research and development challenges.

2 DRDoS attack

In a DRDoS attack, which is a type of DDoS attack, the attacker saturates a target's resources such as networks by generating a vast number of packets by reflecting packets on a number of machines on the Internet and leading those packets to the target. Such an attack is enabled by taking advantages of services with the following two features.

●Amplification effect
This is a server function which can amplify communications. An attacker can amplify the communication volume each time when a packet goes through a server, by using a protocol that creates a response packet whose length is longer than that of the request packet. Such a type of attack is sometimes called an "amplification attack," because it abuses the amplification-effect.

●Reflection effect
This is a server effect in which a server works as a reflector of communication. An attacker can make a server send a response packet to an arbitrary host, by using a protocol that creates a response packet without confirming the sender IP address[*5]. Such a server working as an attack springboard is called a reflector.

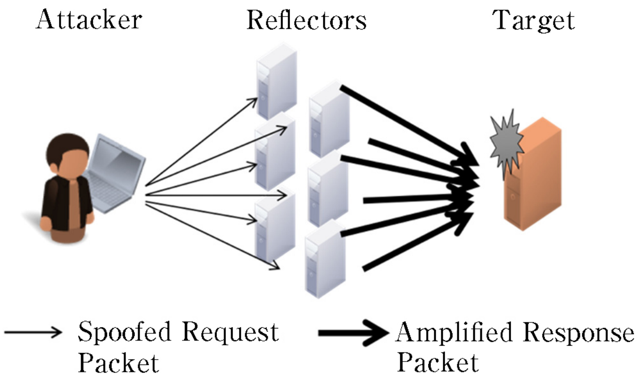

Fig. 1 DRDoS Attack Scheme

Attackers, taking advantages of those features, accomplish their DRDoS attacks by the following procedure (Fig. 1). First, they pick up machines that they can control for generating fake request packets whose sender IP addresses are replaced by the target's IP address so that the packets responding to the fake packets go to the target instead of the actual senders, and make the machines under their control send the fake packets to reflectors—reflectors send their response packets to the target (reflection effects). Furthermore, in such a reflection process, the size of a response packet is larger than that of the request packet (amplification effect). As a consequence, a vast number of packets go to the address of the target. The target's network gets saturated with the packets from reflectors, and at last the target is forced to stop its services.

Reference [7] has reported that, judging from the actual conditions including the estimated number of possible reflectors available and amplification factors, 14 types of protocols including DNS and NTP can be used for DRDoS attacks. Furthermore, other protocols including TCP/3-way handshake reportedly can be used for DRDoS attacks [8]–[11]. As a consequence, the threats of DRDoS attacks are expected to expand.

3 AmpPot (DRDoS honeypot)

Honeypot; This is an information system implemented so that it can be a target of illegal access or other abuses, whose mission is to observe and analyze illegal accesses/access trends (or signs) and identify the illegal access methods. We have been developing AmpPot—a honeypot for DRDoS attacks—aiming to observe DRDoS attacks. AmpPots are placed on the Internet; they make observations/analyses of DRDoS attacks and identify attack means. So, through operating AmpPots on the Internet, we can monitor DRDoS attacks at the level of a reflector that could be used as a springboard.

3.1 Configuration

We can assume that attackers are periodically making search-scans to hunt for reflectors that are available for attacks. It means that we have to design an AmpPot so that it can respond to attackers' request packets but will not take part in actual attacks. For satisfying such requirements, we have configured our AmpPot as shown in Fig. 2. An

[*5] Protocols using UDP (User Datagram Protocol) in their TCP/Transport layer will have such vulnerability.

AmpPot consists of the following three components: “server program”; “access controller”; and “honeypot manager.” The server program sends back a response packet when receiving a request packet. The access controller, working in-between the server program and the Internet, controls communications when the honeypot is used for an attack. The honeypot manager manages/controls the server program and the access controller, sending out the access logs on the honeypot.

3.2 Implementation

As of March 2016, our AmpPots have been installed as shown in Table 1, observing six types of protocols that are considered possibly applicable to DRDoS attacks. We have configured each of our AmpPots in the following way: installing the server program shown in Table 1 on an Ubuntu Server[*12]; as the access controller, installing an iptables[*13]; for the honeypot manager, using our original shell-script-program. Communications are logged in PCAP format by using tcpdump[*14]—an AmpPot sends out those logs packed in a PCAP-format file.

Table 1 List of AmpPot services / implementations

Protocol Name	Port	Implementation
QOTD	17/UDP	quoted[*6]
CHG	19/UDP	xinetd[*7]
DNS	53/UDP	BIND[*8], Unbound[*9]
NTP	123/UDP	NTP Project[*10]
SNMP	161/UDP	Net-SNMP[*11]
SSDP	1900/UDP	Simple Script

3.3 Operation of AmpPot

In Table 2, we list the AmpPots that we are currently operating for our observation. As of March 2016, we are providing 6 types of services and making observations with

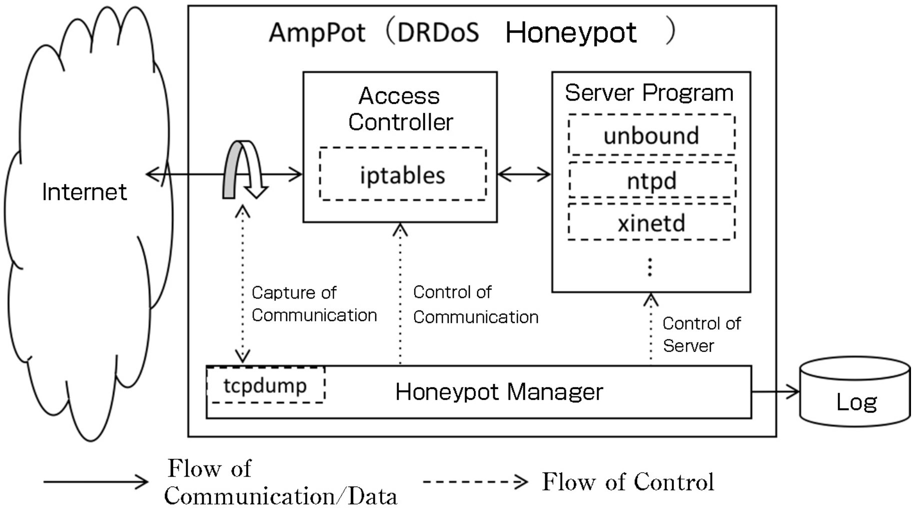

Fig. 2 AmpPot (DRDoS honeypot)

Table 2 Summary of AmpPots in current operation

ID	Date of Installation	Date of Enhancement (the AmpPots whose enhancement dates are not written have been in full operation since the day of installation)
H01	2012/10/06	DNS, CHG (2013/07/26~), QOTD・NTP・SNMP・SSDP (2014/09/25~)
H02	2013/05/13	DNS only
H03	2014/05/13	QOTD・CHG・DNS・NTP, SNMP (2014/09/17~), SSDP (2014/10/03~)
H04	2014/05/13	QOTD・CHG・DNS・NTP, SNMP・SSDP (2014/09/17~)
H05	2014/05/10	QOTD・CHG・DNS・NTP, SNMP・SSDP (2014/10/18~)
H06	2014/05/10	
H07	2014/05/10	

[*6] http://www.mrp3.com/webutil/quoted.html
[*7] http://www.xinetd.org/
[*8] https://www.isc.org/downloads/bind/
[*9] https://www.unbound.net/
[*10] http://www.ntp.org/
[*11] http://www.net-snmp.org/
[*12] http://www.ubuntu.com/
[*13] http://www.netfilter.org/projects/iptables/index.html
[*14] http://www.tcpdump.org/.

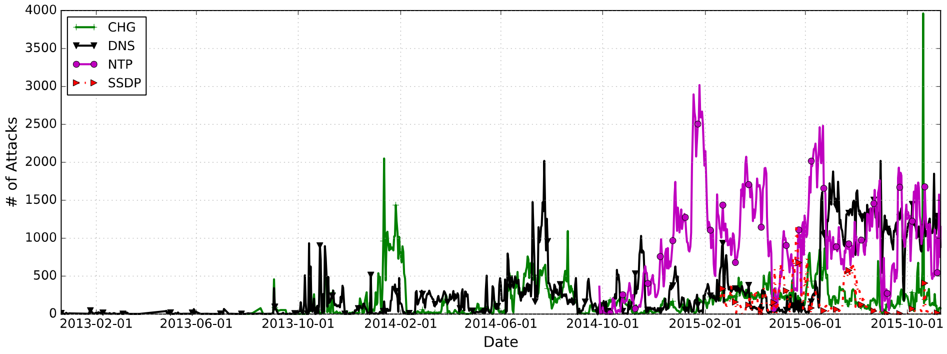

Fig. 3 Trends in the number of attacks (per an AmpPot-sensor)

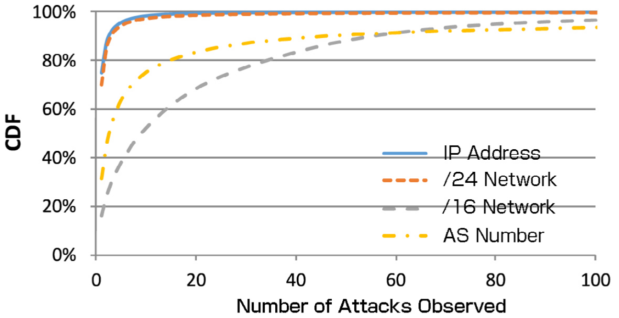

Fig. 4 Distribution of attack repetitions

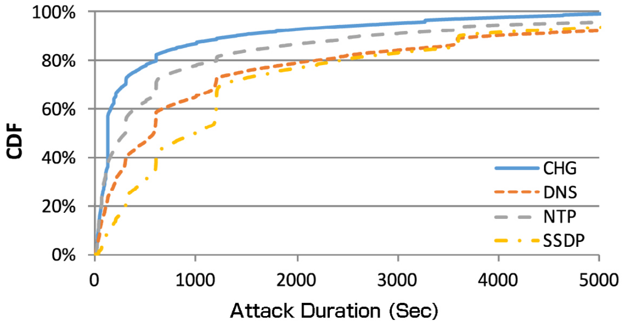

Fig. 5 Distribution of attack duration

7 honeypot sensors. Each of the seven honeypots is installed on the ISP service line, providing general users in Japan with services. Six AmpPots out of the seven—one is dedicated to DNS observation—observe the six-types of protocols shown in Table 1. The first AmpPot started its observation in as early as October 2012; since then, we have enhanced our AmpPot system by adding honeypots and services, as timely as possible to observe a wider range of attacks.

4 Analysis of DRDoS Attacks

In Figure 3, we show the trends in the number of DRDoS attacks (per AmpPot) we have observed. In October 2012, when we started observations, we observed almost no attacks. However, since the second half of 2013, the number of attacks has climbed; in October 2015, 2,600 attacks per day on average were observed. Our analysis of the DRDoS attacks observed in October 2015 on their protocol-by-protocol distribution (share) shows that the following were observed: 76 QOTD attacks per sensor (0.1%), 10,806 CHG attacks (12.9%), 34,457 DNS attacks (40.7%), 37,488 NTP attacks (44.3%), 27 SNMP attacks (0.03%). and 1,656 SSDP attacks (2.0%).

In this section, we present our analysis of the attacks observed in the six months (181 days) from January to June in 2015, focusing on the following three points: how many attacks were observed (“Attack Repetitions” in Subsection **4.1**); how long each attack lasted (“Attack Duration” in Subsection **4.2**); and how many pots observed attacks (“Percentage of Honeypots Observing Attacks” in Subsection **4.3**). In Subsection **4.4**, we make discussions on our analyses. We will focus on the four protocols of CHG, DNS, NTP and SSDP in further discussions, because attacks by the other two protocols of QOTD and SNMP were rarely observed.

4.1 Attack Repetitions

In Figure 4, we show the distribution of attack repetitions which aggregate attacks by IP-address, /24-network, /16-network, or AS-number. The curve in Fig. 4 show that, among the attacks (counted by IP address) during the six months, while 80% received only one attack, only 15% received more than 10 attacks. Another case, where the number of attacks is counted by /24-network, shows a similar trend to that of the case of IP address counting; however, on the other hand, in a /16-network or AS-number-counting case, more than 50% of the attack victims received over 10 attacks in the six months.

4.2 Attack duration

In Figure 5, we show the distributions of attack duration. The attack-duration distributions, while showing slight protocol-to-protocol differences, have their peaks at exact numbers of seconds such as 300, 600, 900, 1,200 or 3,600. Comparisons of the durations for different protocols show the following trends: the duration of CHG attack is the shortest while that of SSDP is the longest. Looking at overall protocols, 18% of attacks lasted for less than 60 seconds, 48% lasted for shorter than 300 seconds, 63% lasted for shorter than 600 seconds, and just 8% lasted for longer than 3,600 seconds.

4.3 Percentage of honeypots observing attacks

Multiple honeypots can simultaneously observe an identical attack, because DRDoS attacks are executed by using a number of reflectors as a springboard. In Figure 6, we show the percentage of honeypots that observed attacks. We found the following facts: with regard to NTP attacks, multiple honeypots observed more than 80% of the attacks; with regard to the attacks that use DNS or SSDP for springboards, a moderate amount—around 40%—of attacks were observed by multiple honeypots,

4.4 Discussions

As stated at the top of this section, at the start of our observation, we rarely observed DRDoS attacks. However, in October 2015, we had 2,500 DRDoS attacks per day.

This is partly because we had enhanced AmpPot observation service, but we can conclude, judging from the trends shown in Fig. 3, that in recent years DRDoS has come to be frequently used as a DDoS attack means. On the other hand, looking into statistics of the number of attacks by services, we found that, while many attacks using DNS or NTP were observed, almost no attacks using QOTD or SNMP were observed. Although this could be partly because some mismatches existed in honeypot implementations or setups, we can conclude that those services were not useful for attackers—attackers were not attracted by those services in terms of the volume of available reflectors on the Internet or the amplification factors.

While AmpPots have observed many DRDoS attacks, as stated in **4.1** and **4.2**, the number of victims that received attacks more than one time, and the attack-duration, looking at the trends, is short. We have not reached a clear conclusion about why such trends were observed. However, an explanation we could provide is that the number of those attacks we observed includes that of trial attacks. DDoS attack service providers called Booter or Stresser are providing trial-attack services or limited (number of attacks or duration) services with free or low prices; that could lead to a large number of attack observations. In addition, from the finding that, as stated in **4.3**, there are many attacks that are not observed but on one honeypot, we can conclude that a certain number of attacks existed, which are not observable by the current seven honeypots. Therefore, we have to prepare the arrangement for increasing the number of observation cases of attack by adding honeypots and finding out how many honeypots are required to observe attacks without a loss.

5 DRDoS-attack alert system

The communications that were captured by AmpPots are highly likely related to illegal communications because AmpPot-services are not open to the public. Therefore, we can formulate a DRDoS-Attack Alert System through collecting and analyzing AmpPot-observed communications to detect DRDoS attacks and sharing such information. In Figure 7, we show the configuration of the proposed DRDoS Attack Alert System. The system consists of the following three components: "Attack Observation Component"; "Attack Analysis Component"; and "Alert Distribution Component." The attack observation component manages and operates AmpPots described in Section **3** to observe DRDoS attacks and delivers its observation log to the attack analysis component. The attack analysis component, extracting necessary information from the communication log, executing analyses, and transfers to the alert distribution component the information of the communication that it judges as an attack. The alert distribution component distributes alerts to registered organizations. For prevent-

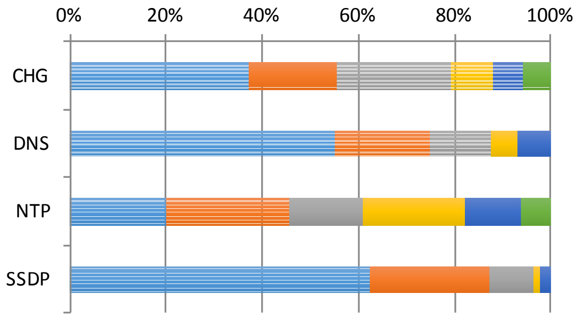

Fig. 6 Percentage of honeypots observing attacks

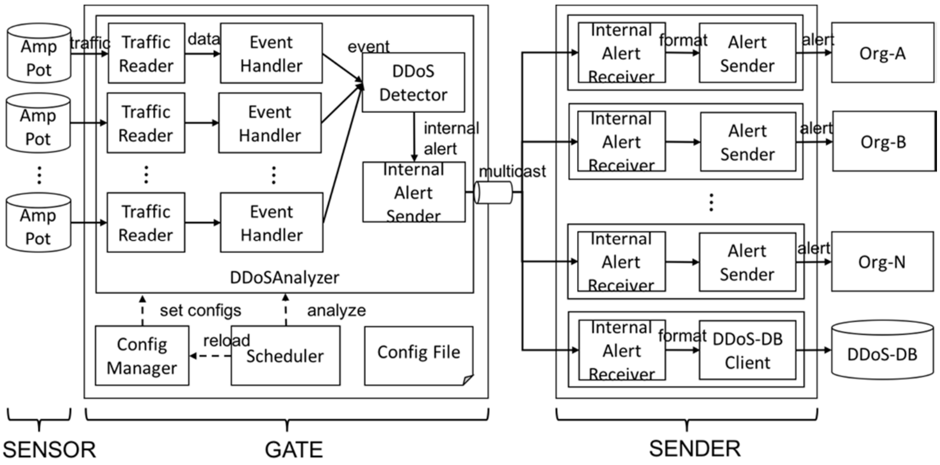

Fig. 7 Configuration of DRDoS-attack alert-system

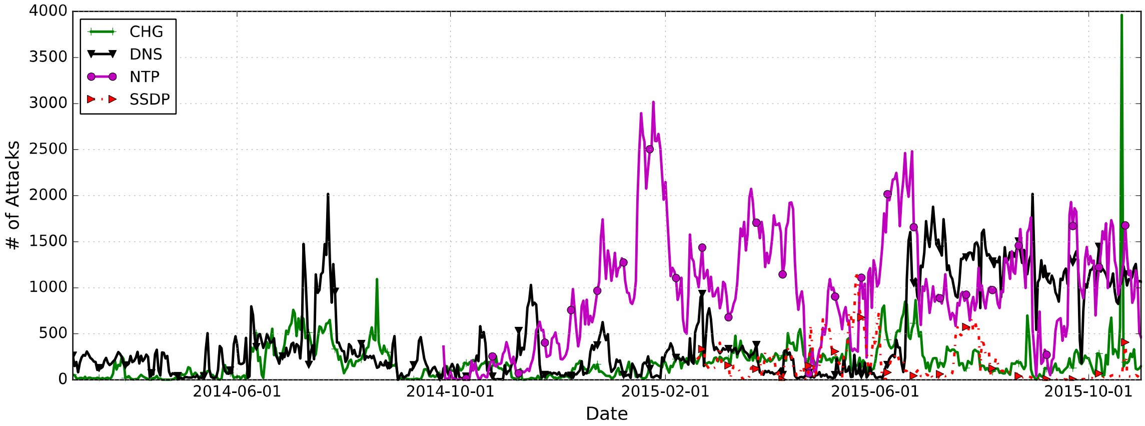

Fig. 8 Trends in the number of alerts delivered by the alert system

ing unnecessary alerts from being delivered, we designed the alert distribution component so that it filters alerts and shapes the alert messages to each of the registered organizations into the format individual organizations request, and furthermore, we use fluentd[*15], which is an open-source log collector, or make an email available for alert delivery.

According to the framework of research and development projects in Japan, we have been operating the system we proposed since February 2014. As of March 2016, we have been delivering DRDoS attack-alert information to a number of organizations in Japan (Fig. 8). AmpPot provides services that are not open to the public, and is able to detect attack communications relatively easily, so AmpPot is expected to provide correct and prompt alerts. Therefore, the alert system we have proposed is promising to assist early countermeasure preparation for DRDoS attacks by providing network operators with alert information.

6 Conclusions

We have provided, in this article, general information on AmpPot which we have researched and developed, shown the results of our analyses of observed DRDoS attacks, and introduced our efforts on a DRDoS attack alert system. We will continue the operations of the AmpPot sensor system, and enhance the system to have the capability of observing a larger number of attacks by adding sensors and protocols. Furthermore, we will go further, beyond just delivering alert information through the DRDoS attack alert system, into regularly analyzing the trends in DRDoS attacks through periodically preparing and distributing attack observation reports. In addition, we will put efforts into investigating the DRDoS attack services such as Booter Services for the details of their operations and infrastructures.

[*15] http://www.fluentd.org/

Acknowledgments

The research and development was partly conducted as a research and development contract in the information and communications field of the Ministry of Internal Affairs and Communications; "Proactive Response Against Cyber-attacks Through International Collaborative (PRACTICE)."

References

1 CloudFlare, "The DDoS That Almost Broke the Internet," http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/, accessed 2016/04/21.

2 Akamai, "DD4BC: PLXsert warns of Bitcoin extortion attempts," https://blogs.akamai.com/2014/12/dd4bc-anatomy-of-a-bitcoin-extortion-campaign.html, accessed 2016/04/21.

3 Jose Jair Santanna, Roland van Rijswijk-Deij, Rick Hofstede, Anna Sperotto, Mark Wierbosch, Lisandro Zambenedetti Granville, Aiko Pras, "Booters - An Analysis of DDoS-as-a-Service Attacks," Integrated Network Management (IM), IFIP/IEEE Symposium, 2014.

4 Jose Jair Santanna, Romain Durban, Anna Sperotto, Aiko Pras, "Inside Booters: An Analysis on Operational Databases," Integrated Network Management (IM), IFIP/IEEE Symposium, 2015.

5 Lukas Krämer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, Christian Rossow, "AmpPot: Monitoring and Defending Amplification DDoS Attacks," Research in Attacks, Intrusions, and Defenses (RAID), Springer International Publishing, pp.615–636, 2015.

6 Daisuke Makita, Katsunari Yoshioka, Tsutomu Matsumoto, "Observing DNS Amplification Attacks with DNS Honeypot," IPSJ Journal, vol.55, no.9, pp.2021–2033, 2014.

7 Christian Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse," Symposium on Network and Distributed System Security (NDSS), 2014.

8 Marc Kührer, Thomas Hupperich, Christian Rossow, Thorsten Holz, "Exit from Hell? Reducing the Impact of Amplification DDoS Attacks," USENIX Security Symposium, (2014).

9 Marc Kührer, Thomas Hupperich, Christian Rossow, Thorsten Holz, "Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks," USENIX Workshop on Offensive Technologies (WOOT), 2014.

10 Default Deny, "MC-SQLR Amplification: MS SQL Server Resolution Service enables reflected DDoS with 440x amplification," http://kurtaubuchon.blogspot.jp/2015/01/mc-sqlr-amplification-ms-sql-server.html, accessed 2016/04/21.

11 The Akamai Blog, "RIPv1 Reflection DDoS Making a Comeback," https://blogs.akamai.com/2015/07/ripv1-reflection-ddos-making-a-comeback.html, accessed 2016/04/21.

Daisuke MAKITA

Researcher, Cyber Tactics Laboratory,
Cybersecurity Research Center
Researcher Graduate School, Yokohama
National University
Cybersecurity

Katsunari YOSHIOKA, Dr. Eng.

Invited Advisor, Cyber Tactics Laboratory,
Cybersecurity Research Center
Invited Advisor, Graduate School, Yokohama
National University
Cybersecurity