NTP Reflection DDoS Attack Explanatory Document

3/13/2015 Edition 1

JANOG NTP Information Exchange WG

ntp-talk-wg@janog.gr.jp

Translation Contributed by SEIKO Solutions Inc.

Table of Contents

1. Overview

This document outlines the issues related to denial of service attacks (NTP Reflection DDoS) launched by exploiting NTP and the methods that can be used to mitigate such attacks.

DoS (Denial of Service) attacks which involve increasing the network traffic (volume), and occupying all the bandwidth to cause denial of service conditions is one of the security issues that has become more visible in recent years. Among them, the DDoS (distributed denial of service) attacks originating from multiple points of origin are known to be difficult issues to resolve because it is difficult to distinguish legitimate user traffic from malicious traffic, and Even if there is the required infrastructure to overcome this vulnerability, the ability to scale of the infrastructure is limited when trying to sustain the networks operation under the volume of the attacks.

DDoS attacks with such features have been observed routinely. However, there have been increasing incidents of attacks exploiting the NTP (Network Time Protocol),since 2013 NTP is the standard protocol for time synchronization over the network, since the year 2013. In this context, we can see that information about the use of NTP to generate effective and broadband DDoS attack was widely known around the world. The effectiveness of these attack techniques has been widely recognized, and the techniques have thus been gaining in popularity. This could lead to greater prevalence of this problem in the future.

On the other hand, there needs to be widespread awareness around the Internet as a whole regarding measures that can be adopted to address the root cause of this problem. However, one cannot say that we have a sufficient repository of information about measures and techniques on how to tackle this issue. While there is a continuing need to spread awareness on this problem, the availability of the required references falls short, and it is difficult to say whether the right information is provided to the people who need it in a manner in which it can be effectively utilized.

This document summarizes the causes and preventive measures that can be utilized by the information systems of corporations and organizations and Internet service providers

(ISP). This document, therefore, introduces and summarizes the measures that can be taken by the person managing the information systems or the engineer in order to mitigate such attacks.

2. Challenges

2.1. Threats of a DDoS attack

2.1.1. Example of an incident that occurred overseas

One of the most notorious DDoS attacks that occurred last year, was the case [1] [2] experienced and reported by CloudFlare during February. The size of the attack appears to have peaked at 400 Gbps, ranking it among the largest DDoS attacks ever observed, in which the attackers exploited the NTP (Network Time Protocol) that performs time synchronization. If we compare this to what was considered to be the largest attack using DNS [3] until this point, the traffic amplification factor was more than 6 times as much per compromised server. In this case, more than 4,529 NTP servers were exploited, and it is said that the average DDoS traffic flow generated per NTP server was 87 Mbps.

Apart from the CloudFlare example, in the example [4] of an online gaming website being attacked, it was also reported that NTP was exploited. Further, based on the research done by Incapsula [5], it is reported that among the techniques that were used for DDoS attacks observed in January and February of 2014, the denial of service attacks caused by exploiting NTP (NTP Reflection DDoS) was one of the main techniques used.

2.1.2. Domestic incident

There have been challenges in obtaining information pertaining to security incidents like DDoS attacks that have occurred in Japan. There are no clear examples publicly available to validate the existence of corporations or organizations that have faced DDoS attacks involving the exploitation of NTP. On the other hand, JPCERT/CC, which receives reports on domestic security incidents involving the Internet, has been reporting and sending alerts [6] that it has been receiving incidents relating to DDoS attacks where the monlist function of ntpd has been abused.

It has come to light that Japanese firms and corporations have also been the target of such DDoS attacks. A Symantec blog [7] suggests that the hacktivist group Anonymous,

which propagates cyber attacks for promoting their social or political agenda, is specifically targeting oil companies with these DDoS attacks. It is no secret that Japanese firms are also victims of this propaganda. Not only this, but there has also been an example [8] of a local online gaming platform that has long been the target of such DDoS attacks.

Consequently, DDoS has been an imminent threat even for domestic information systems, and the likelihood of NTP being exploited as one of the methods used to cause denial of service, which is outlined in this document, has increased significantly in recent times.

2.2. How does the attack work?

In this section, the basis of the DDoS attack mechanism, or in other words how the source address of the UDP packet is spoofed has been described to give a better understanding of how this attack is propagated. Following this, the factors that make NTP especially vulnerable to an attack will been explained.

2.2.1. DDoS attack by spoofing the source address of a UDP packet

The UDP (User Datagram Protocol) widely used over the Internet, is a connectionless protocol, making it particularly vulnerable to source spoofing unless sufficient precautions are taken. The attacker exploits this vulnerability and sends a service request packet based on UDP with a forget address (the victim's) with a forged address to some server (springboard, reflector) thus using the spoofed address of the target as the source address. Because the source address is forged, the unsuspecting target server replies and sends data immediately to the victim. In such cases, when a forged packet elicits a large, overwhelming response, it can cause a massive traffic load to hit the victim's network bandwidth. This is how the DDoS attack, in which the source address of a UDP packet (UDP-based Amplification Attacks [9]) is spoofed, essentially functions.

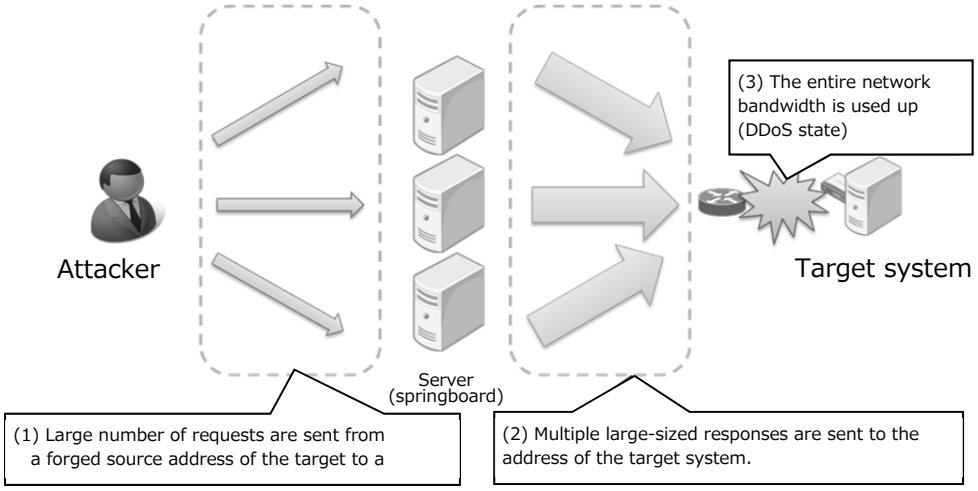

Figure 1 DDoS attack in which the source address of UDP packet is spoofed

2.2.2. Factors making NTP vulnerable

DNS and SNMP have also been prone to DDoS attacks, but the reason why the NTP has been particularly exploited more recently, is due to the fact that the amplification rate is high and there is a large number of servers, placing the attacker in a position of advantage. Table 1 summarizes services vulnerable to DDoS attacks, the amplification rate and the commands that tend to be likely targets for attackers. When the NTP monlist command is exploited, the maximum amplification factor is 556.9 and even the average shows an amplification factor of 200. In contrast to other services, this amplification rate is remarkably high, which goes to show that a bandwidth of a mere 5 Mbps is sufficient to generate a traffic of 1 Gbps, while a bandwidth of only 50 Mbps is sufficient to generate traffic of 10 Gbps.

Protocol	Amplification Factor	Vulnerable Command
NTP	556.9	Monlist
DNS	28 to 54	Any other
SNMP	6.3	GetBulk request

Table 1 Examples of protocol/services that are prone to exploitation (Extract from [9])

Further, the time synchronization function is not only present in the Servers or network devices connected to the network, but also in various other kinds of devices like network printers, network cameras and other systems using NTP. Though these numerous devices are just elements in the total scheme of things, they are still vulnerable, making it easy for attackers to pull off such exploits, and launch full-scale attacks.

This is closely related to the configuration based on the NTP specification. NTP is a hierarchal protocol that uses a high-precision NTP server called Stratum0 as its apex (as shown in Figure 2). What is more, the NTP daemon acts as a client for NTP services running on other devices, It also operates as a Server providing NTP services to other devices simultaneously. Therefore, unless appropriate restrictions are set for each NTP daemon, the services may eventually be provided to an unspecified number of devices. Amongst these, it is the monlist command that is exploited in a DDoS attack and is actually a service that does not need to be provided to most devices. However, due to factors such as an unusual configuration, lack of knowledge on the system administrators part or an incorrect default configuration and so on, there are still a large number of devices present that are vulnerable to this attacks.

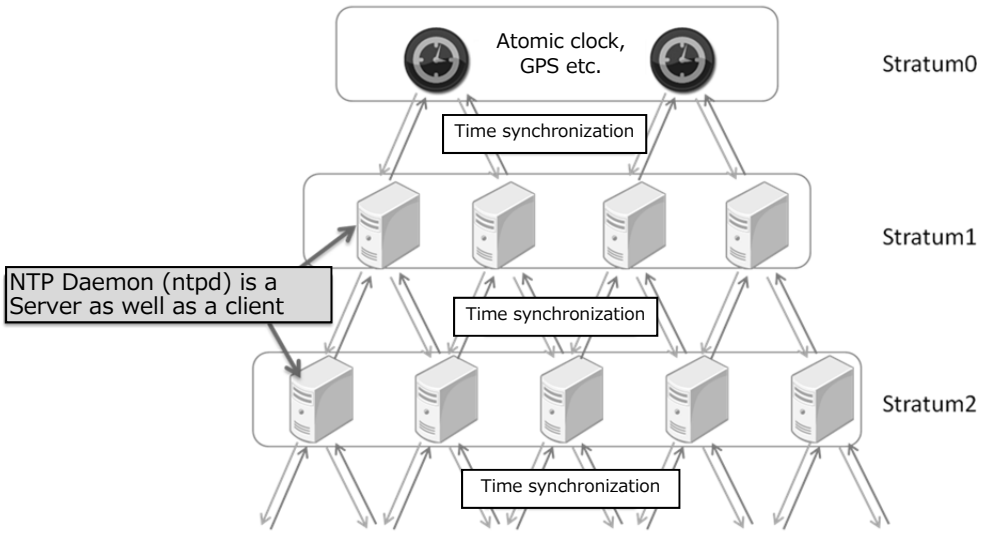

Figure 2 Hierarchal configuration of NTP

3. Mitigation

In this chapter, some technical mitigations, which can be deployed using the available infrastructure of corporations, information systems and internet service providers (ISP) in the event that NTP is exploited to cause a denial of service (via NTP Reflection DDoS), have been outlined. The basic approach would be to address the root cause of this problem, but the kind of measures that can be employed will differ based on each scenario. Figure 3 provides an overall image, and shows the various mitigations that can be taken in different scenarios. The mitigations that can be adopted to safeguard your organization's infrastructure and services in the event of an attack from the victim server (reflector) has been explained in section 3.1, While the measures that can be taken to avoid the misuse of the victim server (reflector) by the attacker to prevent your organization or customer from becoming unwitting participants in reflector and amplification DDoS attacks have been explained in section 3.2.

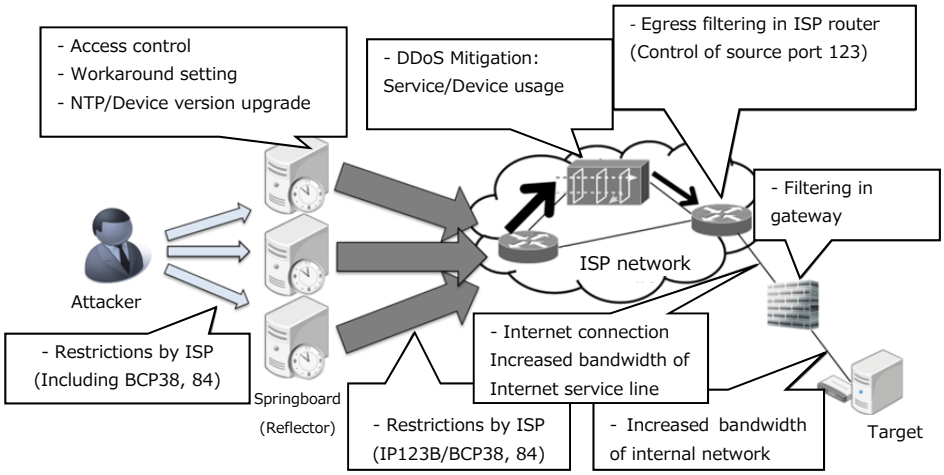

Figure 3 Measures to address denial of service attacks through NTP exploitation (Overview)

3.1. Mitigation - Safeguarding infrastructure and services

3.1.1. Measures that need to be taken by the technician to safeguard the information systems of the organization

Since DDoS is an attack that overloads a service by consuming resources or generating a flood of traffic to overwhelm a target, there are no measures in place to address malicious traffic that exceeds the capacity that a server's resources can handle. Therefore, the bottlenecks need to be identified, and measures should be taken to enhance the resilience of the server in the light of such attacks. In most cases, the entry point is the Internet connection making it the most critical bottleneck, but there are also other factors that need to be looked at in order to address this issue. These have been described in order below.

·Internet service line/internal network bandwidth

Though this method does not address the root cause of the problem, it is largely believed that by having a network with more scalable bandwidth, one can become more prepared to handle the attack. Today, high-speed internet connections of 1 Gbps or 10 Gbps are available at much more affordable prices than before, and so it is advisable to upgrade to such services in order to enhance the resilience of the system.

Further, it is necessary to review the network within the information system. Of late, it is not uncommon to see servers or network devices with interfaces of 1 Gbps or above, but until few years ago, there were a greater number of devices with much less capacity. There have been cases where 100 Mbps or less could be accommodated in cables comprising the network. The bandwidth could be enhanced, but there could be instances where the internal network could become a fresh bottleneck, so it is recommended that the bandwidth of the connections within the local network systems also be checked and enhanced as one of the measures to mitigate this issue.

・Filtering in gateways and ISP routers

One method considered for preventing the inflow of malicious traffic to local networks is the blocking of NTP traffic from non-NTP servers being used for time synchronization at the Internet gateway. More specifically, this would mean filtering the traffic destined for UDP port 123, but it is necessary to check if this will affect communication with remote NTP servers over the Internet, and interfere with the ability to provide outbound NTP services.

Another effective method would be to adopt filtering at the ISP router (Egress Filtering) and make a request to the ISP to restrict massive amounts of NTP traffic over the Internet connection itself. Whether this method can be implemented or not will differ depending on the service policy or the services menu of the ISP. However, in addition to being a preemptive measure, it can serve as a mitigation to counter an actual DDoS attack. Therefore, it is recommended that you build a favorable arrangement by discussing with the concerned ISP manager in advance.

・Implementation of DDoS (Mitigation) service

There are instances where the ISP that you are contracted to could provide services for deploying a specialized set of techniques to resist a DDoS by detecting and mitigating DDoS traffic. Since these issues are addressed in the backbone of the ISP where there is greater bandwidth before entering the clients Internet connection, the expectation is that the malicious traffic over the Internet connection can be addressed as well. However, there could be a considerable gap from the time of DDoS mitigation service subscription until the start of actual service. It is necessary to implement the service beforehand to be able to distinguish the DDoS traffic based on the regular traffic patterns that one is generally aware of.

3.1.2. Measures that can be taken by the Internet Service Provider (ISP) for protecting Customer systems or infrastructure

The actions that can be taken by Internet Service Providers to address this issue are limited to the scope of the communication confidentiality protection clause prescribed in Article 4 of the Telecommunication Business Law. The basic approach has been summarized in "Measures to address large traffic volumes by Telecommunication providers and guidelines for ensuring communication privacy [10]" and this information needs to be referred to as the first step.

These guidelines describe an example of intercepting traffic to UDP port 123 that is used for NTP, and provide for the validity of this approach. However, individual decisions specific to the actual situation at hand need to be taken based on these overall guidelines, and "It is recommended to contact the Ministry of Internal Affairs and Communications in case of any queries". For this reason, a decision needs to be taken regarding the validity of these measures at an individual level, or a consensus needs to be taken within the industry before going ahead with any technical intervention.

3.2. Measures to prevent exploitation - To prevent your organization or the customer from becoming unwitting participants

3.2.1. Understanding the conditions inside the network

Before devising any concrete counter-measures, a thorough understanding of the network that you are managing is essential. An effective way of understanding the network completely is to perform a scan on UDP port 123 inside the network, or utilize the results of the Open NTP Project [11] scan. A service to check for any vulnerable NTP daemons residing inside the specified network has been provided at no additional cost in this project.

There could be instances where the NTP daemon has been enabled due to default settings unintentionally in network devices and the like, and so it would make sense to understand the entire network in addition to the host that is operating as the NTP server.

However, the validity and legitimacy of conducting a scan on the customer’s addresses even though they are within the network managed by your organization was not explained

very clearly when this document was being revised. One needs to be careful while selecting the system to be scanned. In case of any concerns or queries regarding the validity of the system to be scanned or the validity of a method, it is a good idea to contact the Ministry of Internal Affairs and Communications.

3.2.2. Measures that need to be taken by the corporate information system support technician

In order to ensure that the devices or systems being managed do not become unwitting participants in an attack, restrictions can be set in the NTP daemon configuration or in the firewall such that requests are only accepted from known source addresses. The state of the network being managed should be checked, and in case any servers or network devices that can be compromised are identified, it is recommended that measures be taken in accordance with the product specification.

The major challenge in this approach is that there are several variations in the target and so a wide array of methods need to be looked at to address the issue. There are specific counter-measures available with each manufacturer, but there may be products whose support period has expired, making it difficult to deploy basic mitigation techniques like the updating of firmware in such cases. It is recommended that the product be upgraded to the version for which support is available, but interim solutions like controlling the NTP communication end point through packet filtering etc. can be adopted. There are insights available on Cisco IOS, Juniper JUNOS, UNIX ntpd or filters in the template library SECURE NTP TEMPLATE [12] of the NTP related configuration by TEAM CYMRU.

Further, if you are using VPS services or cloud services, there is a possibility that the running server will become one of the reflectors. The basic approach does not change, but in such cases, the carrier assesses the situation by themselves, and recommends a solution to the issue, and it is recommended that you follow their approach.

3.2.3. Measures that need to be taken by the Internet Service Provider

Attacks like the NTP Reflection DDoS that involve spoofing of the source address of the UDP packet cannot be used without allowing the packet with the forged source address on to the network. For this reason, one effective solution would be to carry out filtering

(interception) of the packet with the spoofed source address. While this approach is highly recommended for various reasons, there is still a lack of awareness regarding this method. However, the recent spate of attacks has seen an increased need to ensure that packets with the forged source address are not sent out into the network, and the efforts to addresses this issue are gathering momentum at a global level. The basic approach has been published in RFC2827 (BCP 38) [13] formulated by the IETF, which defines Internet standards. Techniques like packet filtering or uRPF (Unicast Reverse Path Forwarding) that have been published in RFC 3704 [14] have been found to be an effective means of addressing this problem when it actually occurs. A talk given by Matsuzaki at JANOG 18 and 31.5 [15] [16] can serve as an important references.

Further, when a user of your organization has already become part pf a reflection attack, a method to resolve this problem is required. In reality, quite a large number of cases have been observed domestically, where several home broadband routers have been used as pawns in NTP Reflection DDoS attacks to target external systems. In most cases, the home broadband routers are owned by the individual users themselves. There is no other choice but to leave the resolution in the hands of the user in question. For this reason, there is an increasing need for ISP's to invest time and effort in educating users how to handle such situations.

4. Incident Handling

In Chapter 3, we described the specific counter-measures that can be adopted to address the NTP Reflection DDoS issue. At the same time, when faced with this problem, several other steps need to be taken in addition to the measures that have been explained previously. These steps have been consolidated under a process called incident handling, where all the required actions have been summarized. To be more specific, we outline the actions that need to be taken for when your system or your customer's systems are attacked, and when your system or your customer's systems are compromised.

4.1. When your system or the Customer's systems are attacked

4.1.1. Setting the stage

It is not possible to deploy any counter-measures without doing prior preparation. Refer to Chapter 3, and make sure that you are ready and equipped with a strategy well in advance in case the problem were to occur in future. With the scenario, where there is a huge traffic load that exceeds the bandwidth of the Internet connection, it will not be possible to manage this situation without the help of the ISP. That is why it is essential to establish a good rapport with your counterpart in the ISP.

4.1.2. Detect and Act

One of the ways of detecting this problem would be to wait for user's feedback. However, in order to act quickly when faced with a problem, it is recommended that you detect irregularities in a proactive manner through traffic monitoring and service monitoring.

If an attack traffic is detected, and it is within the bandwidth that can be accommodated by the Internet connection, the person responsible for the system can take corrective action. For example, if the origin of the connection is definitive, one of the effective ways to handle this situation, would be to contact the source of this attack traffic and make a request to stem this traffic flow. To ascertain the correct point of contact, one can refer to the WHOIS data for details.

However, when the traffic flow exceeds the bandwidth of the Internet service line, the only option is to have the ISP look into this issue. In such cases, the next step would be to contact the ISP representative and quickly conduct filtering or DDoS mitigation as explained in Chapter 3.

4.2. When your system or the customers systems have been compromised

4.2.1. Setting the stage

In order to understand the situation, it is imperative that traffic visualization and monitoring systems are utilized. Further, when faced with an attack, there may be several instances where you need to contact the respective technical administrator mentioned in the WHOIS data, and so ensure that this WHOIS data is accurate and kept updated at all times.

4.2.2. Detect and Act

Apart from using your own monitoring systems to detect irregularities, the problem may be reported to you by someone from the outside. In case such irregularities have been reported to you from outside your organization, it may be possible that the systems being managed by your organization have been compromised and this may be severely affecting systems in some other location. Therefore, it is important to take these reports seriously and identify the compromised system based on this feedback and check the system. This kind of response will be necessary in the afore-mentioned situation.

Similarly, in case the attack has taken place by forging the source address of the UDP packet, it is possible that you may be the "spoofed source", making you the innocent victim sending out requests to other systems. Therefore, it is very important that you first make sure that "you are not the source of the attack". If the target of the attack is your own systems, take the necessary steps to mitigate the attack. If the problem is with the customer systems, contact the customer by e-mail or phone and have them look into the

issue. In such cases, you need to have prepared the required infrastructure and environment to assist the customer.

In addition, it is also necessary to respond to the individual who has brought this issue to your attention. Basically, since the notifier is also an individual, if he gets the impression that there has been "absolutely no response to his feedback", it will create a completely negative image and such a situation must be avoided as much as possible. To start with, a response like "We are currently monitoring the specified system based on your feedback" is enough. As the next step, once the problem has been identified, it would be a good idea to inform the individual who reported the issue and the party which has fallen prey to this attack that you will give them a status update on the issue within 1 week from the time it was logged as a firmware upgrade may be required for the "specified system in which the issue was reported" as part of the resolution strategy. It will be reassuring for the concerned parties to know that they will soon be hearing from you on further developments on the case. Lastly, it would be good to notify them of the "Support closure" or "Closure plan and schedule" with the help of an incident closure report (Including support plan).

5. Conclusion

It may be because the NTP Reflection DDoS Attack has been known as one of the many ways to launch a DDoS attack that the level of awareness and understanding of this issue is still very low. At the same time, individuals who have observed this traffic load, or individuals who have understood the actual situation through investigation and verification, have begun to realize the seriousness of the issue and are taking the required steps to counter this problem. The abuse of NTP as one of the main protocols in a DDoS attacks is widely rampant as explained in this document.

The effectiveness of these attack techniques has been widely recognized, and the techniques have thus been gaining in popularity. The ease and effectiveness of these attacks will increase the risk of having more such incidents in the future, making the need for a thorough solution to this problem all the more relevant today.

We hope that the contents of this document can serve as important reference material for your organization and for the ongoing efforts on the Internet to counter this problem.

6. Acknowledgment

We take this opportunity to thank the members of the JANOG NTP Information Sharing WG who have made this document possible, and to the members of the JANOG team whose comments and inputs have been so valuable to our initiative. Thank you.

7. Reference documents/URL

[1] CloudFlare, “Technical Details Behind a 400Gbps NTP Amplification DDoS Attack,” 2013. [Online]. Available: http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack.

[2] CloudFlare, “The DDoS That Almost Broke the Internet,” 2014. [Online]. Available: http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet.

[3] CloudFlare, “The DDoS That Knocked Spamhaus Offline (And How We Mitigated It),” [Online]. Available: http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho.

[4] S. Khandelwal, “100Gbps DDoS attack took down Gaming servers with NTP Servers,” 2014. [Online]. Available: http://thehackernews.com/2014/01/ddos-attack-NTP-server-reflection-protection.html.

[5] Incapsula, “Report: 2014 DDoS Trends - Botnet Activity is up by 240%.,” 2014. [Online]. Available: http://www.incapsula.com/blog/ddos-threat-landscape-report-2014.html.

[6] JPCERT/CC, “ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起,” 2014. [Online]. Available: https://www.jpcert.or.jp/at/2014/at140001.txt.

[7] Symantec, “Emerging Threat - Anonymous - Operation Petrol,” 2014. [Online]. Available: http://www.symantec.com/connect/blogs/emerging-threat-anonymous-operation-petrol-june-20-2014.

[8] “DDoS 攻撃で停止の「ファンタシースターオンライン 2」、再開できず 「攻撃規模、極めて大きい」,” 2014. [Online]. Available: http://www.itmedia.co.jp/news/articles/1406/23/news078.html.

[9] US-CERT, “Alert (TA14-017A) UDP-based Amplification Attacks,” 2013. [Online].

Available: http://www.us-cert.gov/ncas/alerts/TA14-017A.

[10] 一般社団法人日本インターネットプロバイダー協会ほか, “電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン,” 2014. [Online]. Available: http://www.jaipa.or.jp/other/mtcs/guideline_v3.pdf.

[11] Open NTP Project, “OpenNTPProject.org - NTP Scanning Project,” [Online]. Available: http://openntpproject.org/.

[12] TEAM CYMRU, “SECURE NTP TEMPLATE,” [オンライン]. Available: http://www.team-cymru.org/secure-ntp-template.html.

[13] D. S. P. Ferguson, “BCP38 Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,” 2000. [Online]. Available: https://tools.ietf.org/html/bcp38.

[14] P. S. F. Baker, “Ingress Filtering for Multihomed Networks,” 2004. [Online]. Available: https://tools.ietf.org/html/bcp84.

[15] M. Yoshinobu, “DNS amplification attacks,” 14 7 2006. [Online]. Available: http://www.janog.gr.jp/meeting/janog18/files/DNSamp_Maz.pdf.

[16] M. Yoshinobu, “BCP38,” 19 04 2013. [Online]. Available: http://www.janog.gr.jp/meeting/janog31.5/doc/janog31.5_dns-open-resolver-maz.pdf.