A Threat of AAAA Resource Record-based DNS Query Traffic

YASUO MUSASHI,† RYUICHI MATSUBA,† and KENICHI SUGITANI †

†Center for Multimedia and Information Technologies, Kumamoto University,
2-39-1 Kurokami, Kumamoto-City, 860-8555, JAPAN

Abstract: We statistically investigated DNS query traffic in a crashed DNS cache server for an IPv4/IPv6-based E-mail server as a spam relay in a university campus network. The interesting results are summarized, as follows: (1) We observed big traffic from the E-mail server when having a spam relay attack from the local hijacked spam bot, and (2) in the DNS query traffic, we can observe a large-scale AAAA resource record (RR)-based DNS query traffic in which the DNS traffic takes almost the same as the A RR-based traffic. Therefore, it can be concluded that the AAAA RR-based traffic becomes a threat for the DNS server in the campus network or the internet.

1. Introduction

It is of considerable importance to keep security of a domain name system (DNS) server because the DNS server plays an very important role to convert a fully qualified domain name (FQDN) into an IP address (a standard resolution), an IP address into an FQDN (Reverse resolution), and a domain name into an FQDN of the authorized SMTP (E-mail) server, and these DNS functions are called in initial stages of the almost major network applications. If the DNS server crashes, the network services in the site are probably disappeared from the internet.

The IPv6 supported network applications gradually but surely increase, for instance, almost the operating systems (OSs) and Web browsers,[1-2] and the recent mail transfer agents (MTAs), are correspondence to the IPv6 network. On the other hand, Toyono *et al.* recently pointed out that increase of the AAAA resource record (AAAA RR)-based DNS query traffic would become one of the big threats on the internet.[3]

Very recently, a DNS cache server for a local E-mail server in a campus network was crashed when the E-mail server was a spam relay that was caused by a local spam bot at August 20th, 2006.

The present paper discusses (1) on traffic analysis of the A and AAAA RRs-based DNS query packet access from the campus network toward the top domain DNS (**tDNS**) server, and (2) traffic analysis of the A and AAAA RRs-based DNS query packet access from the local E-mail server.

2. Observations

2.1 Network systems

We investigated traffic of DNS query accesses among the top domain DNS server (**tDNS**), ‡ the local DNS cache server, the DNS clients in the campus network, and a local E-mail server in which the postfix-2.1.5-4.2.RHEL4 is employed.[2] Figure 1 shows a schematic diagram of a network observed in the present study. **tDNS** is one of the top level domain name system servers and plays an important role of subdomain delegation and domain name resolution services for many PC terminals.

2.2 DNS Query Packet Capturing

In **tDNS**, BIND-9.2.6 program package has been employed as a DNS server daemon.[4] The DNS query packets and their contents have been captured and decoded by a query logging option (see

†Center for Multimedia and Information Technologies, Kumamoto University.

‡**tDNS** is a top domain DNS server in a certain university and the OS is Linux OS (kernel-2.4.33), and hardware is an Intel Xeon 2.40GHz Dual SMP machine.

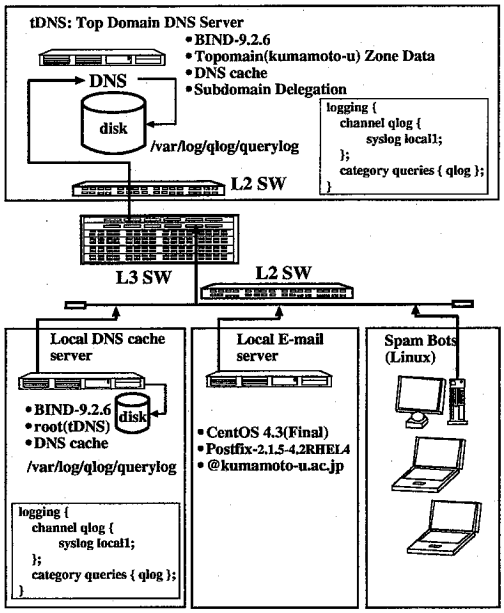

Figure 1. A schematic diagram of a network observed in the present study.

man named.conf), as follows:

```
logging {
        channel qlog { syslog local1; };
        category queries { qlog; };
}
```

The log of DNS query traffic has been recorded in the syslog file which are daily updated by the crond system. The syslog messages mainly consist of a host domain name (an address resource record; A RR for IPv4 and AAAA for IPv6), an IP address (a pointer RR; PTR RR), and mail exchange (an MX RR).

2.3 AAAA RR-based DNS Query Traffic in Campus Network

We observed traffic of DNS query request packet access from the campus network and the top domain DNS server (**tDNS**) through September 1st, 2005 to August 31st, 2006. In Figure 2, the A resource record (RR)-based DNS query traffic is usually much greater than the AAAA RR-based one. However, the situation changes drastically

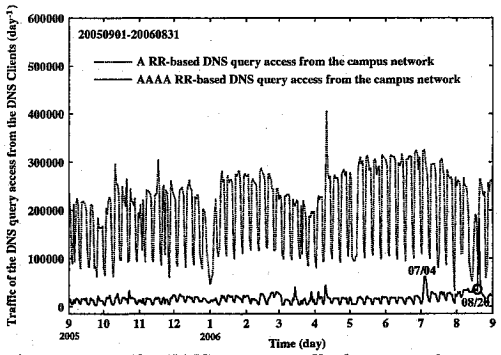

Figure 2. The DNS query traffic between the top domain DNS server and the DNS clients in the campus network through September 1st, 2005 to August 31st, 2006. The solid and dotted lines show the A and AAAA resource record (RR)-based DNS query traffics, respectively (day^{-1} unit).

at August 20th, 2006. After this day, the AAAA RR-based DNS query traffic considerably increases in the same manner or a little bit greater than the A RR-based DNS query traffic. Secondarily, we can observe a significant peak in the AAAA RR-based DNS query traffic curve at July 4th, 2006, in Figure 2. In this day, we updated the new local E-mail server as CentOS 4.3 + Postfix-2.1.5-4.2.RHEL4 from Solaris 2.6 + Postfix-2.0.6.

Therefore, we further investigated statistically on the AAAA RR-based DNS query traffic at the day of August 20th, 2006.

3. Results and Discussion

3.1 Top DNS Query Clients

We carried out statistics on the AAAA resource record (RR)-based DNS query traffic from the DNS clients in the campus network and the results are demonstrated, as below:

133.95.a1.a2	163,609
133.95.b1.b2	13,235
133.95.c1.c2	873
133.95.d1.d2	797
133.95.e1.e2	412

The top is a local E-mail server and the second is its local DNS cache server. Usually, the direct DNS query traffic from the local E-mail server

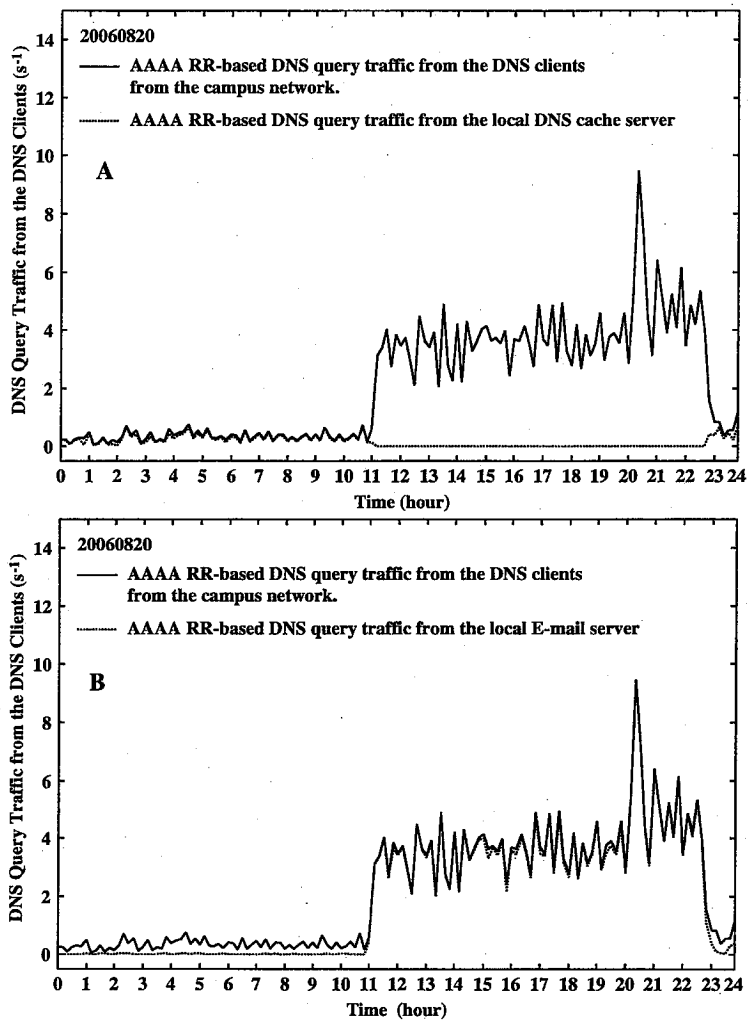

Figure 3. The AAAA resource record (RR)-based DNS query traffic between the top domain DNS server and the DNS clients in the campus network through August 20th, 2006. Both solid lines show the AAAA RR-based DNS query traffics from the DNS clients and the dotted lines of Figures 3A and 3B demonstrate the DNS query traffics from the local DNS cache server and the local E-mail server, respectively (s^{-1} unit).

to the top DNS (**tDNS**) server does not take place. This is because the resolver configuration file (/etc/resolv.conf) in the E-mail server consists of only two IP addresses in which the local DNS cache server (the default) and the **tDNS** server (optionally, if the default failed).

However, the direct DNS query access from the E-mail server to the **tDNS** one can take place so that this result indicates that the local DNS cache server cannot react or reply to the DNS query access from the local E-mail server. In fact, the local DNS server stopped through 11:07-23:07 at August 20th, 2006.

We illustrate the total AAAA resource record (RR)-based DNS query traffic curve, the AAAA RR-based DNS traffic curves from the local DNS cache server and the E-mail server in Figure 3.

In Figure 3A, the AAAA RR-based DNS query

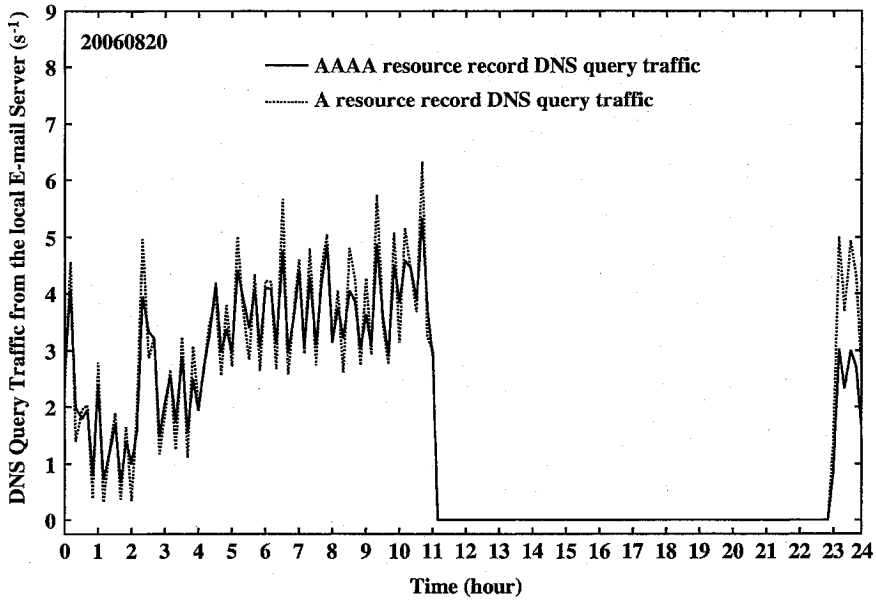

Figure 4. The DNS query traffic between the local DNS cache server and the local E-mail server in the campus network through August 20th, 2006. The solid and dotted lines show the AAAA and A resource record (RR)-based DNS query traffics, respectively (s^{-1} unit).

traffic from the local DNS cache server changes simultaneously with the total AAAA RR-based DNS traffic, however, it stops at 11:07 and starts again after 23:07. In Figure 3B, the DNS query traffic from the local E-mail server synchronizes well with the total DNS query traffic.

As a result, it can be clear that the local DNS cache server stopped August 20th, 2006. Therefore, we need to investigate the local DNS server, and the DNS query traffic between the local DNS server and the local E-mail server.

3.2 Analysis of DNS Cache Server

We statistically investigated on the DNS query traffic between the local DNS server and the E-mail server through August 20th, 2006, as shown in Figure 4.

In Figure 4, the A resource record (RR)-based DNS query traffic curve resembles well the AAAA RR-based DNS query traffic one from 00:00 to 11:07. The both DNS query traffics stop at 11:07 and restarts at 23:07.

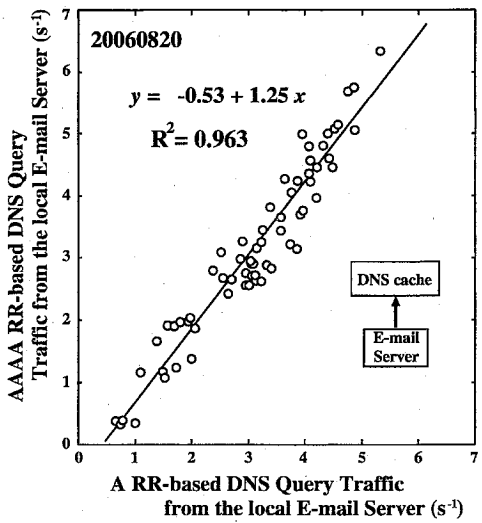

Figure 5. The A resource record (RR)-based DNS query traffic from the local E-mail server versus the AAAA RR-based DNS query traffic from the local E-mail server through 00:00-11:07, August 20th, 2006 (s^{-1} unit).

Surprisingly, the total DNS query traffic takes a rate of 343,418 packet/day in which the lost DNS traffic (11:07-23:07; 12 hours) is ignored. If the

local DNS cache server worked ceaselessly, the total DNS query would probably take *ca.* 687,000 packet/ day (the usual rate; 300,000 packet/day). The traffic rate consists of the A, AAAA, PTR, MX, and TXT RRs-based traffic ones of 133,303, 139,794, 13,942, 35,474, and 16,681 packet/day, respectively. This feature indicates that the total DNS query traffic from the local E-mail server is mainly driven by the A and AAAA RRs-based DNS query traffics.

Figure 5 shows regression analysis on the A resource record (RR)-based DNS query traffic from the local E-mail server versus the AAAA RR-based DNS query traffic from the local E-mail server. The data are 00:00-11:07 August 20th, 2006. The correlation coefficient (R^2) is calculated to be 0.963. This means that the AAAA RR-based DNS query traffic is probably synchronized with the A RR-based DNS query traffic *i.e.* the AAAA and A RRs-based traffic can take place simultaneously.

Furthermore, we investigated statistically on the syslog file (/var/log/maillog) for the local E-mail server and the following five top SMTP clients are observed, as

127.0.0.1	9769	loop back
133.95.f1.f2	5194	spam bot
133.95.g1.g2	483	authorized
133.95.h1.h2	255	authorized
133.95.i1.i2	141	authorized

where the top SMTP client is an IP address for loop back *i.e.* it means the local E-mail server itself, and the second top is one of the unauthorized SMTP clients that is a hijacked Linux OS-installed PC and it works as a spam bot. On the other hand, we had been already found the PC in August 2nd, 2006 with employing the new our bot worm (BW) detection method.[5]

Interestingly, the second top SMTP traffic takes a rate of 5,194/day is very suspicious because the other authorized SMTP clients take even only 100-500/day. This feature means that the E-mail server is used as a spam relay by the spam bot.

Here, we can know a reason why the big DNS query traffic occurs by the local E-mail server. Also, the anti spam and/or virus filter is installed in the local E-mail server, and the E-mail server program package with the spam/virus filter like SpamAssasin,[6] Postgrey,[7] and Clam Anti Virus,[8] considerably generates much DNS query traffic. Furthermore, the local E-mail server is natively corresponding to IPv6 based network application/environment so that it provides an environment that can easily generate the undesirable AAAA RR-based DNS query traffic.

4. Concluding Remarks

We performed statistical analysis on the DNS query traffic from the crashed DNS cache server to the top DNS (**tDNS**) server and the DNS query traffic between the local DNS cache server and the local E-mail server as a spam relay in the campus network. The following results are obtained, as follows: (1) In August 20th, 2006, the DNS query from the local DNS cache server to the **tDNS** server stopped through 11:07-23:07 and the DNS query traffic were directly requested from the local E-mail server. (2) The both DNS query traffics mainly consist of the A and AAAA RRs-based DNS query traffics. This is because the E-mail server is corresponding to the IPv6 networks. Conventionally, a standard domain name resolution are carried out with requesting only an A RR-based DNS query packet. This means that in the case of the E-mail server, if it corresponds only to the IPv4 networks, probably, no the AAAA RR-based DNS query traffic occurs *i.e.* the DNS query traffic would become a half of the present standard name resolution traffic and the local DNS cache server could work without any crash. However, since the IPv6-ready network application is currently spreading, we should pay hereafter considerable much attention to the AAAA RR-based DNS query traffic in the campus/enterprise network or the internet.

Acknowledgement. All the calculations and investigations were carried out in Center for Multimedia and Information Technologies

(CMIT), Kumamoto University. We gratefully thank to all the CMIT staffs and system engineers of MQS (Kumamoto) for daily supports and constructive cooperations.

References and Notes

1) http://www.mozillar.org/

2) http://www.postfix.org/

3) http://www.nanog.org/mtg-0602/-ishibashi.html

4) http://www.isc.org/products/BIND/

5) A. Ludeña Romaña, D., Nagatomi, H., Musashi, Y., Matsuba, R., and Sugitani, K.: A DNS-based Countermeasure Technology for Bot Worm-infected PC terminals in the Campus Network, *Journal for Academic Computing and Networking*, Vol. 10, No.1, pp.39-46 (2006).

6) http://spamassassin.apache.org/

7) http://isg.ee.ethz.ch/tools/postgrey/

8) http://www.clamav.net/