Detection, Prevention, and Managements of Security Incidents in a DNS Server

Yasuo Musashi,[†] Ryuichi Matsuba,[†] and Kenichi Sugitani[†]

[†]*Center for Multimedia and Information Technologies, Kumamoto University,*
2-39-1 Kurokami, Kumamoto-City, 860-8555, JAPAN
[†]*{musashi, matsuba, sugitani}@cc.kumamoto-u.ac.jp*

Abstract

We have developed a new distributed denial-of-service (DDoS) attack detection-, prevention-, and management-system (DPMS) for the DNS server. This system gives us much helpful information to understand what kinds of security incidents take place in the networks.

1. Introduction

It is well-known that the DNS server provides very important information such as a fully qualified domain name (an FQDN, an A record, standard access), an IP address (a PTR record, reverse access), and a mail exchange (an MX record) to DNS clients like E-mail server (SMTP/POP3) and/or WWW browsing network applications. In other words, these network applications strongly depend on the DNS server. From this point, the DNS query packets provide us very important information at initial stages of the network applications like, for example, the looking Web sites by the Web browser, and the IP addresses of the PC clients and the FQDN of the E-mail servers by SMTP server daemon program. These applications are deeply related to many recent security incidents like mass mailing worm-infection and/or pre-scanning for a distributed denial-of-service (DDoS) attack to the network servers. Therefore, observing traffic of DNS query packets probably provides us much useful information of the security incidents and gives much knowledge to develop an intrusion detection/prevention system (IDS/IPS) [1-7]. Rikitake et al. have reported that the DNS server can be one of the IDS components [8]. Also, we have reported that we can detect IP addresses of the mass mailing worm (MMW)-infected PC clients by observing the MX record based DNS query packets from the PC clients and developed the detection- and prevention-system against the PTR record based DNS query DDoS attack [9,10].

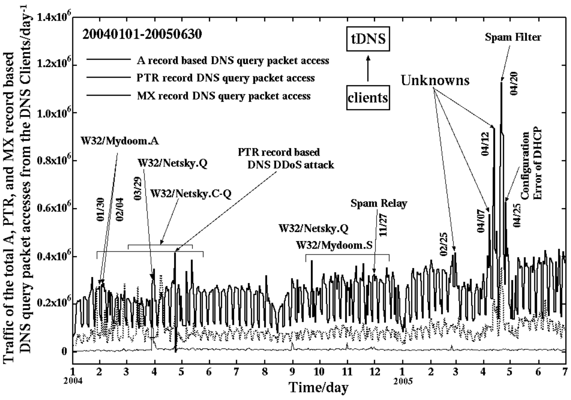
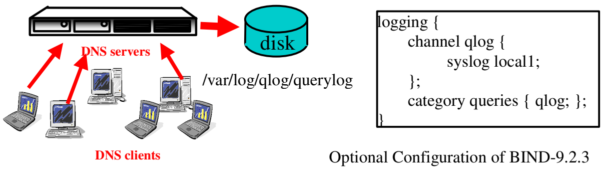


Figure 1. The DNS query traffic between the top domain DNS (tDNS) server and the DNS clients through January 1st, 2004 to June 30th, 2005. The thick solid line shows the A record based DNS query packet access, the dotted line indicates the PTR record based DNS query packet access, and the thin solid line demonstrates the MX record based DNS query packet access (day^{-1} unit).



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

Optional Configuration of BIND-9.2.3

Figure 2. A schematic diagram of a network observed in the present study.

Recently, the top domain name system (DNS) server of a university has been under several DNS query packet-based DDoS attacks like transmitting various kinds of DNS query packets, probably because in order to crash the DNS server, to search the FQDNs, the FQDNs of E-mail servers, and the IP addresses of the next victim PC clients, and to be a base of DoS attack. Especially, traffic of the A record based DNS query packets to the top domain DNS server of the university was abnormally increased during the late days of February and the days of April, 2005 (see Figure 1).

The present paper discuss (1) on the investigation of three different kinds of DDoS attacks through February 25th, April 7th, and 12th, 2005, (2) on correlation analysis of the A record based DNS query packets traffic between the DNS server and the DNS clients that especially transmit strange query contents of the A record based

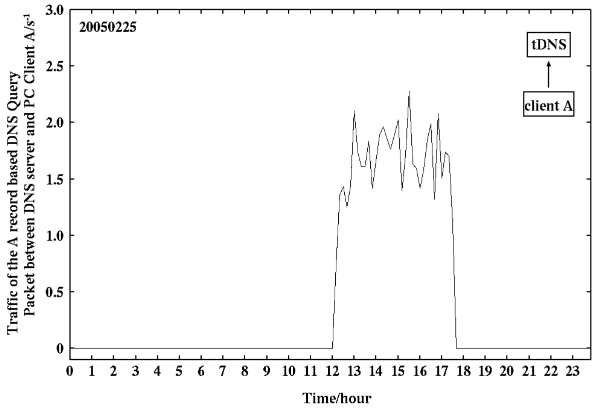


Figure 3. The traffic of the A record based DNS query packet access between the top domain DNS (tDNS) server and the DNS client A at February 25th, 2005 (s^{-1} unit)

DNS query packets including fully qualified domain names (FQDN) of E-mail servers and IP addresses directly, (3) how to implement a DNS query packets-based DDoS attack detection- and prevention-system into the DNS server, (4) how to manage the results in detection- and prevention of the DDoS attacks, effectively.

2. Observations

2.1 Network systems

We investigated traffic of DNS query accesses between the top domain DNS server (**tDNS**) and the DNS clients. Figure 2 shows an observed network system in the present study and optional configuration of the BIND-9.2.3 DNS server program daemon[12] of the **tDNS**. The **tDNS** is one of the top level domain name (kumamoto-u) system servers and plays an important role of domain name resolution and subdomain name delegation services for many PC clients and the subdomain networks servers, respectively, and the operating system is Linux OS in which kernel-2.4.30 is currently employed with the Intel Xeon 2.0GHz dual CPU system, the 1GB core memory, and Intel 100Mbps EthernetPro Network Interface Card.

2.2 Capture of DNS Query Packets

In **tDNS**, BIND-9.2.3 program package has been employed as a DNS server daemon[12]. The DNS query packets and their contents have been captured and decoded by a query logging option (Figure 2, see % man named.conf in more detail). The log of DNS query access has been recorded in the syslog files. All of the syslog files are daily updated by the crond system. The line of syslog message mainly consists of the content of the DNS query packet like a time, a source IP address of the DNS client, a fully qualified domain name (an A record type), an IP address (a PTR record type), and mail exchange (an MX record type).

1		2		3		4		5	
m	9975	ma	7506	mai	7404	mail	7399	mail.	5894
s	1569	mx	1883	smt	872	smtp	872	smtp.	491
p	566	sm	888	mx1	583	mx1.	451	mail1	229
a	542	in	265	mx0	402	rela	195	mailh	201
c	490	re	237	mx.	378	mx2.	167	mail2	200
i	462	po	231	rel	196	inbo	134	relay	190
n	403	ns	153	mx2	171	spam	101	mailg	162
b	395	sp	143	inb	134	mx01	92	inbou	133
r	363	co	132	pop	118	www.	91	mail-	129
e	341	ba	120	spa	108	serv	79	mails	108
				www	96	mx3.	79	smtp1	96
				bar	85	pop.	76	mx01.	90
				ser	82	barr	73	mail0	74
				mx3	82	post	69	barra	73
				pos	75	emai	67	smtp-	72
				mx-	70	gate	64	serve	70
				gat	67	filt	51	email	67
				ema	67	mx0.	49	mail3	65
				cor	62	mx4.	47		
				web	57				
				ns.	55				
				mta	55				

Figure 4. Statistics of the query contents for the A record based DNS query packets from the client A at February 25th, 2005.

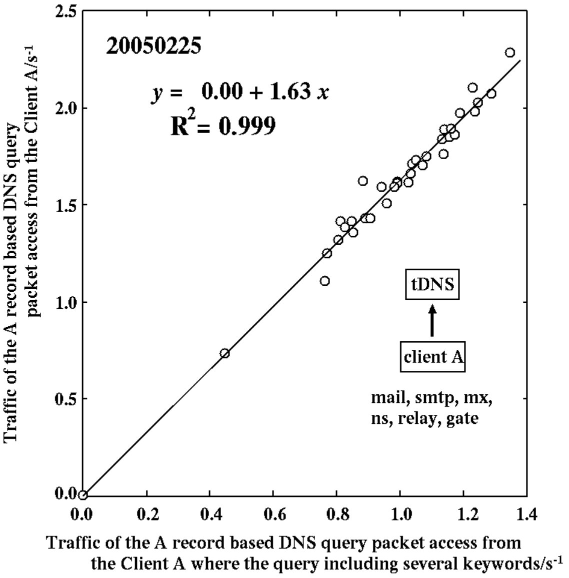


Figure 5. Total traffic of the A record based DNS query packet access from the client A versus traffic of the A record based DNS query packet access from the client A including the six keywords at February 25th, 2005 (s^{-1} unit).

2.3 Abnormal Traffic of the A Record based DNS Query Access from the Client A

Firstly, we observed traffic of the A record based DNS query packets from a DNS client A to the top domain DNS (**tDNS**) server through the day of February

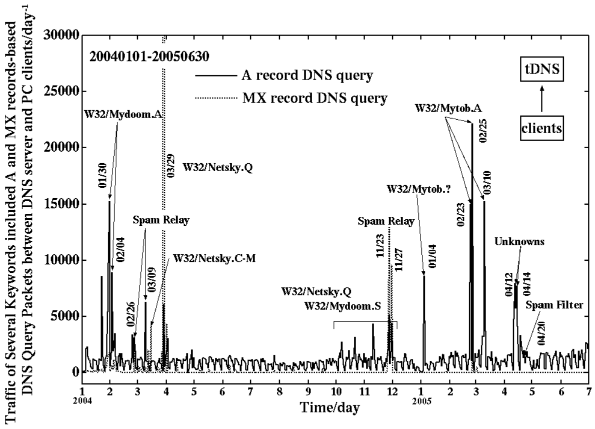


Figure 6. Total traffic of the A record based DNS query packet access including the six keywords ("mail", "smtp", "mx", "ns", "relay", and "gate") in the top domain DNS server (tDNS) through January 1st to 2004 to June 30th, 2005 (day^{-1} unit)

25th, 2005 (Figure 3), because the client A is one of the top DNS query access clients at the day.

In Figure 3, the traffic starts from 12:00 and ends after 17:30 since we filtered this DNS query access. The numbers of the total DNS query packets, the A record based DNS query packets, and the PTR record based ones, are obtained to be 32,728day^{-1}, 32,721day^{-1}, and 7day^{-1}, respectively, and no MX record based DNS query packet can be observed. This result shows that the total DNS query access traffic from the client A almost consists of the A record based DNS query packets access.

We can demonstrate statistics of the contents for the A record based DNS query packets from the client A at February 25th, 2005 (Figure 4). In Figure 4, the keywords of "mail", "smtp", "mx", "ns", "relay", and "gate" are used to generate fully qualified domain names of the E-mail servers that have ever been observed when detecting IP addresses of the W32/Mydoom.A or W32/Mydoom.S mass mailing worm (MMW)-infected PC clients[9,11] *i.e.* the PC client A is probably infected with a new type of mass mailing worm (MMW) which resembles well W32/Mydoom.A or W32/Mydoom.S MMW. This new worm was assigned to be the W32/Mytob.A bot worm (BW) after February 27th, 2005 by several anti-virus vendors [13].

Why do the W32/Mydoom.A-S MMWs and the W32/Mytob.A BW decrease sending the MX record based DNS query packet access? This is because SMTP process needs the DNS solution twice: one is a mail exchange resolution (sending the MX record based DNS query packet) to get an FQDN of the E-mail server and the other is standard resolution (sending the A record based DNS query packet) to convert the FQDN into an IP address. In order to save the time for the former MX resolution as possible, the W32/Mydoom.A or W32/Mydoom.S MMW is improved to complete or convert the harvested generic domain name from the PC hard disk drive into the FQDN.

client B		client C	
0.0.0.0	26	***.***.y****.com	12
.**-u.ac.jp	13	www.*****m.com	7
133.9*.**.192	11	yahoo.co.jp	6
133.9*.**.73	10	www.****.****.co.jp	6
133.9*.**.66	9	mail.****.com	6
133.9*.**.64	9	img.****.co.jp	5
133.9*.**.52	9	i.****.jp	5
133.9*.**.89	6	ai.****.jp	5
mil.***.********-u.ac.jp	5	133.9*.***.194	5
.**.*****-u.ac.jp	5	133.9*.20*.2**	5
2**.*.2**.*8	5	127.0.0.1.***-u.ac.jp	5
133.9*.**.9	5	127.0.0.1	5
133.9*.**.8	5	relay.****.net	4
133.95.**.7	5	rd.*****.co.jp	4

Figure 7. Statistics of the contents for the A record DNS query packets from the clients B and C at April 7th and 12th, respectively.

Figure 5 shows regression analysis on the total traffic of the A record based DNS query packet access from the client A versus the traffic of the A record DNS query packet access from the client A in which the six keywords of "mail", "smtp", "mx", "ns", "relay", and "gate" are included. The data is February 25th, 2005. In Figure 5, the correlation coefficient (R^2) is 0.999. This means that the traffic of the A record based DNS query packet including the six keywords strongly correlates with the abnormal traffic of the A record based DNS query packets from the client A.

From this point, we have further investigated on the traffic of the A record based DNS query packet access that includes several keywords consisting of head characters in the FQDNs for E-mail servers.

3. Results and Discussion

3.1 Query Content-based Scanning

We illustrate the observed total traffic of the A record based DNS query packet access including the six keywords ("mail", "smtp", "mx", "ns", "relay", and "gate") and the MX record based DNS query packet access from the PC clients without any Web/E-mail servers through January 1st, 2004 to June 30th, 2005, as shown in Figure 6. Interestingly, we can find several new peaks of, for instance, January 22nd (hijacked PC), February 23rd (W32/Mytob.A), March 9th (spam relay), and 23rd (W32/Mytob.A), and April 14th (Unknown), 2005. Surprisingly, the largest peak for traffic curve of the A record DNS query packets access at April 20th, 2005 (Figure 1), disappears considerably (Figure 6), probably because in the day, a lot of DNS resolving accesses from the internet in order to get the FQDNs/DNs or their IP addresses of the subdomain E-mail servers as a spam relay in the university. Also, the peak at April 12th, 2005, is unexpectedly smaller than that in Figure 1 and the peak at April 7th, 2005, disappears. From these results, we need, therefore, to investigate further on the unknown two peaks at April 7th and 12th, 2005.

The clients B and C are the top DNS query access clients (229,309day^{-1} and 400,964day^{-1}) that belong to each of peaks at April 7th and 12th, 2005, respectively, and statistics for their query contents are shown in Figure 7. In Figure 7, we can clearly notice that IP addresses are directly described in the query contents in spite of the A record based DNS query packets. Usually, query contents of the A record DNS query packets only include fully qualified domain names (FQDNs). The number of IP addresses are calculated to be 161,329 (70.4%) and 200,645 (50.0%) for the days of April 7th and 12th, respectively.

Figure 8 demonstrates regression analysis on the total traffic of the A record based DNS query packet access from the clients B and C versus traffic of the A record based DNS query packet access from the clients B and C including the IP addresses. The data are April 7th and 12th, 2005 and the correlation coefficients (R^2) are 0.994 and 0.999 for clients B and C, respectively. This means that the total traffic of the A record based DNS query packet access from the clients strongly correlates with the traffic of ones that include directly IP addresses as their query contents. In other words, this feature is useful to detect the abnormal traffic of the A record based DNS query packet access from the PC clients.

We illustrate the observed traffic of the A record based DNS query packets including IP addresses directly from the PC clients of the university, as shown in Figure 9. In Figure 9, we can reproduce the abnormal traffic of the A record DNS query packets that include IP addresses directly at April 7th and 12th, and we also find new peaks at April 11th, 15th, May 10th, June 7th, and 9th, 2005.

As a result, it is clear that (1) the query contents for the recent abnormal traffic of the A record based DNS query packets mainly include the six keywords ("mail", "smtp", "mx", "ns", "relay", and "gate") and/or directly IP addresses, (2) the abnormal traffics strongly correlate with the total traffic of the A record based DNS query packets, and (3) this feature can be useful for detecting abnormal traffic of the A record based DNS query packets from the PC clients that are infected with or hijacked by the bot worm like W32/Mytob.A or its variants.

3.2 ADPS of DPMS

The DPMS is a total systematic name for the IDS/IPS for DNS server consisting of several detection systems, a prevention system, and a management system, which has been installed into the top domain DNS (**tDNS**) server in the university[9,10]. We designed and developed new detection-, prevention-, and management-system (DPMS) against the recent abnormal traffic of the A record based DNS query packet access that include the six keywords and IP addresses directly as their query contents (ADPS). The prevention system of the new system (ADPS) is the same as the previously reported system of PTRDPS[10]. The detection system of the ADPS checks the syslog messages (including client source IP addresses and their query contents by an optional configuration of BIND-

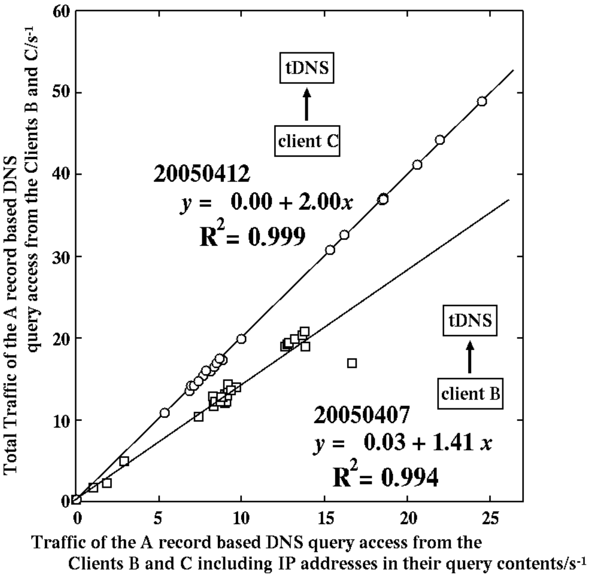


Figure 8. Total traffic of the A record based DNS query packet access from the clients B and C versus traffic of the A record based DNS query packet access from clients B and C including the IP addresses at April 7th and 12th, 2005 (s^{-1} unit)

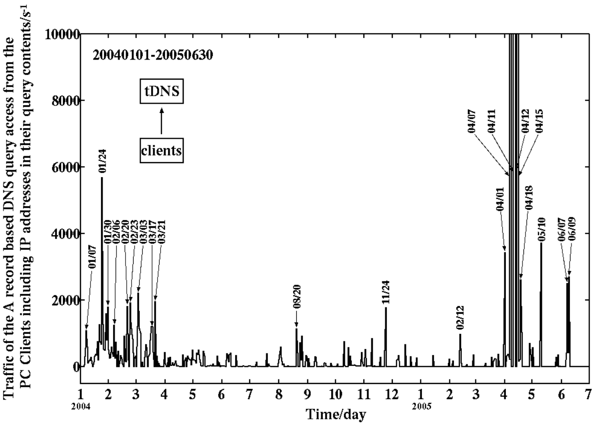


Figure 9. Total traffic of the A record based DNS query packet access including IP addresses to the top domain DNS (tDNS) server through January 1st to 2004 to June 30th, 2005 (day^{-1} unit)

9.2.3[12], see Figure 2) of the DNS server program daemon with the six keyword in the head word of an FQDN or an IP address as "A.B.C.D" (A, B, C, and D are a digit number: 0-255) in the query contents of the A record based DNS query packets. The sampling rate for each client source IP address is arbitrarily fixed in a time per one hour. When the traffic becomes greater than the threshold (=500 h^{-1}), it can be concluded that the client source IP addresses are suspicious. Then, the IP addresses are sent to the prevention system (an IP address based filtering system) and the management system (a database and E-mailing systems). This ADPS has joined into the DPMS *i.e.* has been installed into the top domain DNS (**tDNS**) server of the university after the day of April 25th, 2005 and the abnormal traffic of the A record based DNS query packets has been decreased after the day (see Figure 6 and 9).

4. Concluding remarks

We statistically investigated syslog files of the top domain DNS (**tDNS**) server in a university when observing abnormal traffic of the A record based DNS query packet access and we have finally obtained results that the abnormal traffic are detectable because the six keywords and/or IP addresses themselves are included in the query contents of the A record based DNS query packets. Based on these results, we have developed and installed the new detection-, prevention- and management-system (DPMS with ADPS) into the **tDNS**, and we are currently testing it. Also, we started to investigate on the peaks of May 10th, June 7th, and 9th (an IP address representation was found in several PTR based DNS query packets from the PC clients; usually, IP address "A.B.C.D" should be described as "D.C.B.A.in-addr.arpa"), and on the reason why the total traffic of the A record based DNS query packet access is still gradually increasing (Figure 1).

Acknowledgement

All the studies were carried out in CMIT of Kumamoto University and M-Lehrstuhl in Johann Wolfgang Goethe Universität of Frankfurt am Main. We gratefully thank to all the CMIT staffs and Professor Dr. K. Rannenberg, and this study is a grant aid of Promoting Advanced Educational Program (2004) for Overseas Dispatch and GP by the Ministry of Education, Culture, Science and Sport.

References

[1] S. Northcutt and J. Novak, *Network Intrusion Detection,* 2nd ed; New Riders Publishing: Indianapolis (2001).

[2] D. E. Denning, "An Intrusion-detection model", *IEEE Trans. Soft. Eng.*, Vol. SE-13, No.2, 1987, pp.222-232.

[3] B. Laing: How To Guide-Implementing a Network Based Intrusion Detection System, http://www.snort.org/docs/iss-placement.pdf, ISS, 2000.

[4] B. Mukherjee, L. Todd, and K. N. Heberlein, "Network Intrusion Detection", *IEEE Network*, Vol.8, No3, 1994, pp.26-41.

[5] S. A. Hofmeyr, A. Somayaji, and S. Forrest, "Intrusion Detection Using Sequences of System Calls", *Computer Security*, 1998, pp.151-180.

[6] D. Anderson, T. F. Lunt, H. Javitz, A. Tamaru, and A. Valdes, "Detecting unusual program behavior using statistical component of the Next-generation Intrusion Detection Expert System (NIDES)", *Computer Science Laboratory*, 1995, SRI-CSL-95-06.

[7] http://www.snort.org/

[8] K. Rikitake, H. Nogawa, T. Tanaka, and S. Shimojo, "Behavioral Analysis of DNS and TCP Connections, Computer Security Symposium 2003 (CSS2003), IPSJ Symposium Series, Vol. 2003, No. 15, 2003, pp.521-526.

[9] R. Matsuba, Y. Musashi, and K. Sugitani, "Detection of Mass Mailing Worm-infected IP address by Analysis of Syslog for DNS server", *IPSJ Technical Reports, Distributed System and Management 32nd*, Vol. 2004, No.37, 2004, pp.67-72.

[10] Y. Musashi, R. Matsuba, and K. Sugitani, "Development of Automatic Detection and Prevention Systems of DNS Query PTR record-based Distributed Denial-of-Service Attack", *IPSJ Technical Reports, Distributed System and Management 34th*, Vol. 2004, No.77, 2004, pp.43-48.

[11] http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYDOOM.A

[12] http://www.isc.org/products/BIND/

[13] http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYTOB.A