2007－DSM－45 (17)
2007／5／11

Threats of Unusual DNS Query Traffic from NIS Clients

Dennis A. LUDEÑA ROMAÑA†, Hirofumi NAGATOMI†, Yasuo MUSASHI††, Ryuichi MATSUBA††, and Kenichi SUGITANI††

† Graduate School of Science and Technology, Kumamoto University 2–39–1, Kurokami, Kumamoto, 860–8555 Japan

†† Graduate School of Science and Technology, Kumamoto University 2–39–1, Kurokami, Kumamoto, 860–8555 Japan

Abstract We statistically investigated on unusual DNS query traffic from the several Linux PC servers employing network information system (NIS) as their authentication in the campus network of a university. The following results are obtained: (1) The DNS query traffic includes specific keywords of database servers in which one database is as a NIS server and the others are its NIS clients. (2) The DNS query traffic takes place when the NIS server crashes because recent NIS is carried out with libwrap that performs the name resolution. This name resolution is usually achieved with referring to a /etc/hosts or to the DNS server. Therefore, we can reasonably take a workaround to avoid the unusual DNS query traffic when configuring the specific keywords and their IP addresses in the /etc/hosts file.

Key words DNS based Detection, NIS server, NIS clients

1. Introduction

It is of considerable of importance to keep security of a domain name system (DNS) server because the DNS server plays a very important role to convert a fully qualified domain name (FQDN) into an IP address (a standard resolution), an IP address into an FQDN (a 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 internet network application. If the DNS server crashes, the network services in the site are virtually disappeared from the internet.

Very recently, a primary DNS server in a campus network received unusual DNS query packet traffic from a local site in the campus network through January 14th to 15th and March 11th to 13th, 2007 (see Figure 1). In Figure1, we can observe a significant peak in the total DNS query traffic at January 15th, 2007, and the peak is mainly driven by the DNS query traffic from the campus network. In this day, the top DNS server totally received a recordable 1,282,085 DNS query packet traffic consisting of 964,501 and 317,584 packets for the traffic from the inside and outside of the campus network, respectively.

Previously, we reported similar unusual DNS query traffic from the outside of the campus network in which a lot of unique source IP addresses were found in their packet query contents and this unusual traffic was caused by the spam bot in the campus network [1].

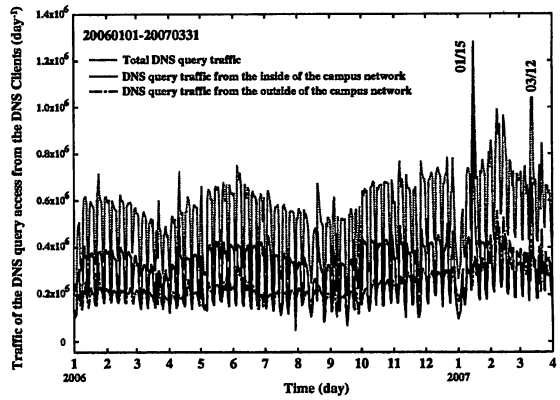

Fig. 1. Traffic of the DNS query packets to the top domain DNS server (**tDNS**) and the traffic from the inside- and the outside-DNS clients in a university through January 1st, 2005 to December 31st, 2005 (day^{-1} unit).

In this paper, we discuss on (1) the investigation of the unusual DNS query packet traffic at January 15th, 2007, mainly, and (2) show a countermeasure technology against the unusual DNS query packet traffic.

2. Observations

2.1 Network System

We investigated traffic of DNS query accesses between the top domain DNS server (**tDNS**) and the DNS clients. Figure

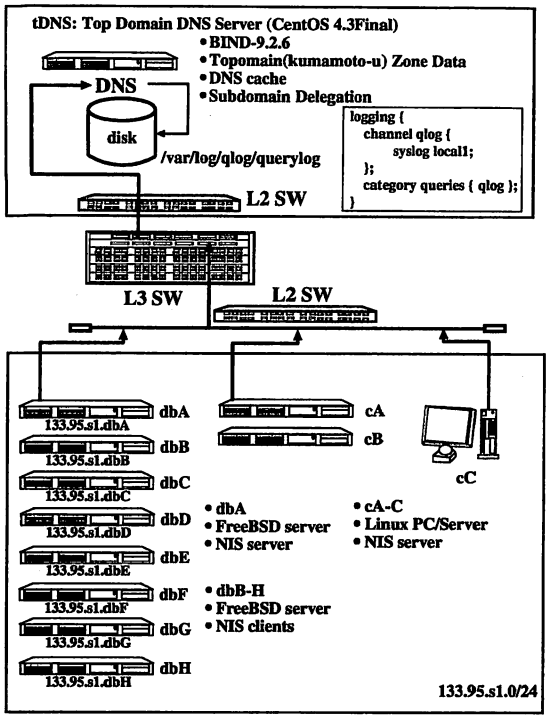

Fig. 2. A schematic diagram of a network observed in the present study.

2 shows an observed network system in the present study and optional configuration of the BIND-9.2.6 DNS server program daemon [2] of the **tDNS** server. The **tDNS** server 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 (CentOS 4.3 Final) in which kernel-2.6.9 is currently employed with the Intel Xeon 3.20 GHz Quadruple SMP system, the 2GB core memory, and Intel 1000Mbps EthernetPro Network Interface Card.

2.2 DNS Query Packet Capturing

In **tDNS**, BIND-9.2.6 program package has been employed as a DNS server daemon [2]. 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 (A and AAAA resource record (RR) for IPv4 and IPv6 addresses, respectively) type, an IP address (PTR RR) type, and a mail exchange (MX RR) type.

2.3 Statistics of DNS Clients

Firstly, we can demonstrate statistics the source IP address of the unusual top three DNS query packet traffic at January 15th, 2007, as follows:

133.95.s1.a1 (cA)	198,585
133.95.s1.b2 (cB)	147,375
133.95.s1.c3 (cC)	146,828

Interestingly, these DNS clients are Linux PCs that they employ the same Linux distribution as Vine Linux 4 which are widely accepted by Japanese Linux users [3]. Therefore, let us name these DNS clients as client A (**cA**), B (**cB**), and C (**cC**), respectively, and from above described results, we have carried out further investigation on the DNS query packet traffic from the **cA**, hereafter.

3. Results and Discussion

3.1 Top DNS Query Contents

We carried out statistical analysis on the query contents in the DNS query traffic from the client A (**cA**) in January 15th, 2007. We can show full statistical results on the DNS query contents, as below:

dbD.FQDN	9968
133.95.s1.dbD	9967
dbF.FQDN	9941
133.95.s1.dbB	9937
133.95.s1.dbF	9932
dbE.FQDN	9931
dbB.FQDN	9930
133.95.s1.dbE	9925
133.95.s1.dbG	9923
dbG.FQDN	9922
133.95.s1.dbC	9922
dbH.FQDN	9920
dbC.FQDN	9916
133.95.s1.dbH	9912
133.95.s2.m1	4

Surprisingly, the query contents the DNS query traffic from the **cA** consist of database servers (**dbA-dbH**) in the same LAN as that of the **cA**. The database servers employ FreeBSD as their OS. And at first, it is likely that the **cA** and the database servers are independent each other, however, they have a point in common, *i.e.* they employ network information system (NIS) [4], [5].

Interestingly, no "dbA.FQDN" can be found in the above statistical results. This result probably means that the **dbA** stopped at January 15th, 2007. In order to check this assumption, we tried to investigate on the syslog message file "/var/log/messages" in the **cA** since the NIS related system messages are usually recorded in the files. Expectedly, a lot of NIS related messages can be observed in the

"/var/log/messages" files, as follows:

```
Jan 15 00:00:00   cA  portmap[11709]: connect from\
133.95.s1.dbD to callit (ypserv): request from\
unauthorized host
Jan 15 00:00:05   cA  portmap[11709]: connect from\
133.95.s1.dbC to callit (ypserv): request from\
unauthorized host
Jan 15 00:00:05   cA  portmap[11709]: connect from\
133.95.s1.dbG to callit (ypserv): request from\
unauthorized host
```

.
.
.

Furthermore, we illustrate the observed DNS query traffic from the client A (**cA**) in January 15th, 2007, as shown in Figure 3.

In Figure 3, the DNS query traffic can be observed constantly, taking almost a rate of 2.3 s^{-1} until 16:50, while the syslog message traffic becomes an almost zero value after 17:52. At this point, these features should be discussed later. Also, interestingly, we can expectedly observe both traffic curves that change in a same manner. Therefore, it can be clearly concluded that the unusual DNS query traffic from the **cA** is dominated by the NIS related syslog messages in the **cA** (the same situation can be observed in the syslog message files in the other clients **cB** and **cC**).

3.2 A Countermeasure Method

We configured directly the hostnames (**dbA-H**) and their fully qualified domain names (FQDNs: **dbA-H.FQDN**) of the database servers into the "/etc/hosts" files in the **cA**, **cB**, and **cC** at 16:50 January 15th, 2007. After 16:50, as shown in Figure 3, the usual DNS query traffic clearly disappears. In the same day, we also rebooted the **dbA** as NIS server at 17:52. After 17:52, the NIS-related syslog message traffic is quickly stopped. This is because the recent NIS employs an IP address-based authentication with a TCP_Wrapper application programming interface (API) library as *libwrap* [6] and the name resolution process is performed referring to the */etc/nsswitch.conf* file in the Linux server or PC. If the configuration term "hosts:" is set to "files dns" in the */etc/nsswitch.conf* file, the */etc/hosts* is employed preferentially to the name resolution *i.e* no DNS query are taken place after this configuration.

Unfortunately, we observed unusual DNS query packet traffic through March 11th to 13th, 2007, again. In March 12th, 2007, the total DNS query traffic is estimated to be 1,043,357 DNS query packets in which the total traffic consists of 694,818 and 348,539 packets of traffics from the inside and outside of the campus network, respectively. Also, we statistically investigated on the DNS query traffic from the

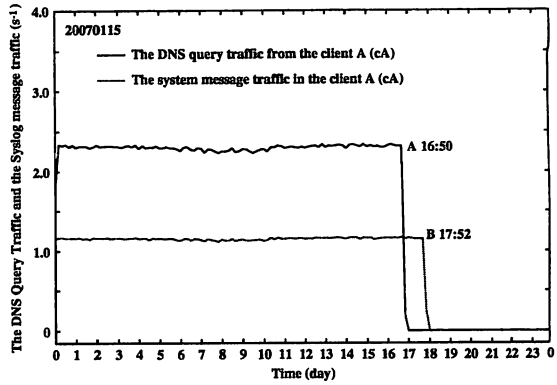

Fig.3. The DNS query traffic from the DNS client A (**cA**) to the top DNS server (**tDNS**) and the syslog message in the **cA** in the day of January 15th, 2007. The solid and dotted lines show the DNS query traffic from the **cA** and the syslog messages traffic in the **cA** (s^{-1} unit).

campus network in the day of March 12th, 2007, and found a top DNS query client D (**cD**) taking a value of 119,314 day^{-1}) in which the full statistical results are obtained, as below:

dbD.FQDN	14312
133.95.s1.dbD	14312
dbF.FQDN	14295
133.95.s1.dbF	14295
dbE.FQDN	14287
133.95.s1.dbE	14287
dbB.FQDN	14285
133.95.s1.dbB	14285
dbG.FQDN	14284
133.95.s1.dbG	14284
dbC.FQDN	14280
133.95.s1.dbC	14280

Expectedly, the query contents of the DNS query traffic from the **cD** consist of the same database servers (**dbB-dbG**) and no query keyword "dbA.FQDN" also can be found in the above results. Actually, the database server A (**dbA**) crashed through March 11th to 13th, 2007.

We can demonstrate the total DNS query traffic from client D (**cD**) and its syslog messages traffic through March 11th to 13th, 2007, as shown in Figure 4. In Figure 4, it is found that the DNS query traffic takes almost a rate of 2.0 s^{-1}, which started from 06:10 March 11th and stopped after 18:13 March 13th, 2007. Also, we configured directly the hostnames (**dbA-H**) and their FQDNs (**dbA-H.FQDN**) of the database servers into the */etc/hosts* file in the **cD** at 18:13 March 13th, 2007. Therefore, it can be concluded that the */etc/hosts* file is very useful to suppress unfavorable unusual DNS query traffic from the UNIX or UNIX-like *host* like Linux- and/or FreeBSD-installed PC clients.

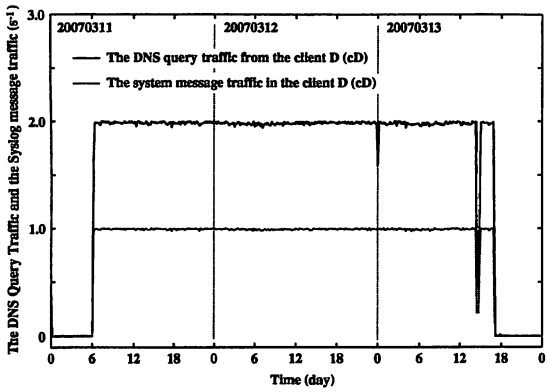

Fig.4. The DNS query traffic from the DNS client A (**cD**) to the top DNS server (**tDNS**) and the syslog message in the **cD** through March 11th to 13th, 2007. The solid and dotted lines show the DNS query traffic from the **cD** and the syslog messages traffic in the **cD** (s^{-1} unit).

4. Concluding Remarks

We have carried out statistical investigation on the unusual DNS query traffic from the Linux servers/PCs clients in the campus network of a university. Interestingly, the query contents in the unusual DNS traffic includes several keywords that are related with several database servers in which the OS is employed FreeBSD 4 and their authentication is employed the network information system (NIS). Furthermore, NIS clients send broadcast packets when searching their NIS servers. This packet broadcasting probably repeated between NIS server and clients and the other Linux server/PCs. As a result, the top domain DNS (**tDNS**) server is faced to severe situation to receive the unusual DNS query traffic. We can suggest a classical workaround employing "/etc/hosts" file and we started to develop automated detection system for the unusual DNS query traffic generated by NIS related incident.

Acknowledgement

All the studies were carried out in CMIT of Kumamoto University. We gratefully thank to all the CMIT staffs.

References

[1] (a) Y. Musashi, S. Hayashida, R. Matsuba, K. Sugitani, and K. Rannenberg Detection- and Prevention System of DNS query-based Distributed Denial-of-Service Attack, Proceedinghe 8th Asia-Pacific Network Operations and Management Symposium Toward Managed Ubiquitous Information Society (APNOS2005), Okinawa, Japan, pp.207-211, 2005.

[2] BIND-9.2.6: Internet Systems Consortium, http://www.isc.org/products/BIND/

[3] Vine Linux 4, http://www.vinelinux.org/

[4] Sun Microsystems, Inc., SunOS Reference Manual, 1990.

[5] Sun Microsystems, Inc., NIS+ and DNS Setup and Configuration Guide, 1995.

[6] Wietse Z. Venema, Eindhoven University of Technology, ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.-tar.gz