Crash of NIS Server Generates Unusual DNS Query Traffic

Dennis Arturo Ludeña Romaña, Hirofumi Nagatomi, Yasuo Musashi,† Katsunori Taniguchi,†† Nobuaki Oomura,†† Ryuichi Matsuba,† and Kenichi Sugitani†

Graduate School of Science and Technology, Kumamoto University,
2-39-1 Kurokami, Kumamoto-City, 860-8555, JAPAN
{dennis,nagatomi}@cs.kumamoto-u.ac.jp

†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

††Faculty of Engineering, Kumamoto University,
2-39-1 Kurokami, Kumamoto-City, 860-8555, JAPAN
††{katsunori.taniguchi,nobuaki.oomura}@eng.kumamoto-u.ac.jp

Abstract

We investigated statistically on the unusual DNS query traffic from the several DNS clients like Linux servers and/or PC terminals in the campus network of a university. The interesting results are: (1) The DNS query traffic includes several keywords relating with database servers in the local area network, to which the Linux servers and PC terminals are belonging. (2) These keywords are generated by network information system (NIS) server program daemons in the database servers. Recent NIS communication employs the remote procedure call (RPC) with libwrap that performs name resolution to the DNS server. From these results, we can reasonably take a workaround to refrain the unusual DNS query traffic when configuring host domain names and their IP addresses in the /etc/hosts file.

1. Introduction

It is of considerable of 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 (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 major network applications on the internet. If the DNS server crash occurs, the network services in the site, will be virtually disappeared from the internet.

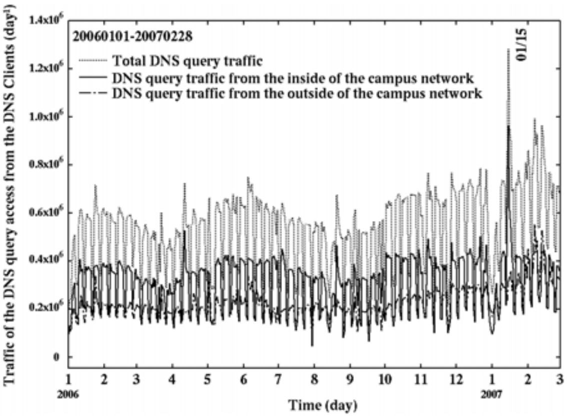

Figure 1. The DNS query traffic between the top domain DNS (**tDNS**) server and the DNS clients through January 1st, 2006 to February 28th, 2007. The dotted line shows the total DNS query traffic, the solid line demonstrates the traffic from the campus network, and the other line indicates the traffic from the outside of the campus network (day^{-1} unit).

Recently, a primary DNS server in a campus network received unusual DNS query packets based traffic from a local site in the campus network through January 14th to 15th, 2007 (see Figure 1). In Figure 1,

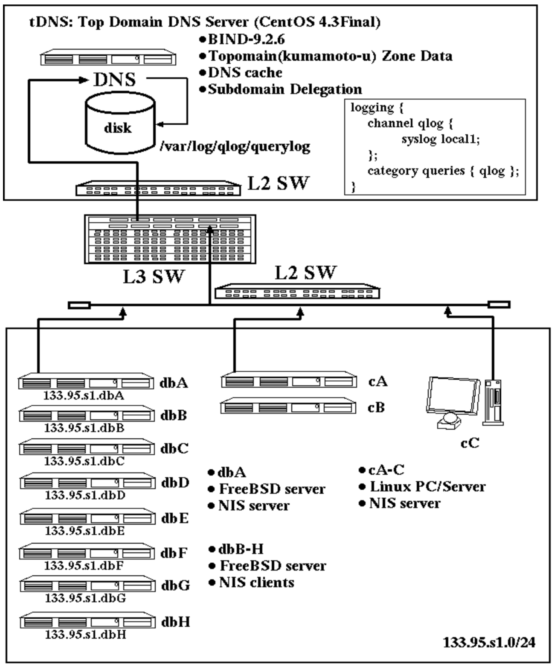

Figure 2. A schematic diagram of a network observed in the present study.

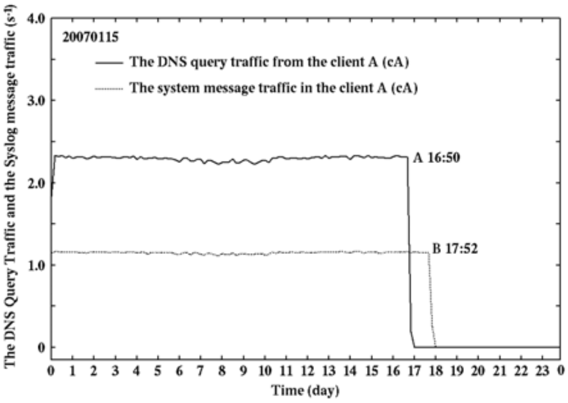

Figure 3. The DNS query traffic from the DNS client A (**cA**) to the top DNS server (**tDNS**) and the syslog message in the **cA** in the day of January 15th, 2007. The solid and dotted lines show the traffic from the **cA** and the syslog message traffic in the **cA** (s^{-1} unit).

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 packets 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 headers and this unusual traffic was caused by several spam bots in the campus network [1].

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

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-9.2.6 DNS server program daemon [2] 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 (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 Package 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
```

These query packets shows some interesting results, 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.

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. The top DNS Query Contents

We begin carrying 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) [3, 4].

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.hostname portmap[11709]: connect from 133.95.s1.dbD to callit (ypserv): request from unauthorized host
Jan 15 00:00:05 cA.hostname portmap[11709]: connect from 133.95.s1.dbC to callit (ypserv): request from unauthorized host
Jan 15 00:00:05 cA.hostname 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 $2.3s^{-1}$ 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

As shown in Figure 3, 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, 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*" 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 in the **cA** (**cB** and **cC**).

4. Concluding Remarks

We have carried out 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) [3,4]. Furthermore, NIS clients send broadcast packets when searching their NIS servers. This packet broadcasting probably repeated between NIS server and clients like other Linux server/PCs. As a result, the top domain DNS (**tDNS**) server is faced to severe situation to receive the unusual DNS query packets based 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 security incidents.

5. Aknowledgment

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

6. References

[1] Y. Musashi, S. Hayashida, R. Matsuba, K. Sugitani and K. Rannenberg, "Detection- and Prevention System of DNS query-based Distributed Denial-of-Service Attack", Proc. the 8th Asia-Pacific Network Operations and Management Symposium Toward Managed Ubiquitous Information Society (APNOS2005), Okinawa, Japan, pp.574-585 (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

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

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