DNS Based Detection of SSH Dictionary Attack in Campus Network

Dennis A. Ludeña Romaña,[†] Yasuo Musashi,[‡] Kazuya Takemori,[†]
Masaya Kumagai,[†] Shinichi Kubota,[‡] Kenichi Sugitani,[‡]
Tsuyoshi Usagawa,[†] and Toshinori Sueyoshi[†]

[†]*Graduate School of Science and Technology, Kumamoto University,*
Kumamoto-City, 860-8555, JAPAN
{dennis, kazuya}@st.cs.kumamoto-u.ac.jp

[‡]*Center for Multimedia and Information Technologies, Kumamoto University,*
Kumamoto-City, 860-8555, JAPAN
musashi@cc.kumamoto-u.ac.jp

Abstract

We statistically investigated the DNS query access traffic from a university campus network toward the top domain DNS (**tDNS**) through March 14th, 2009, when the hosts in the campus network were under inbound SSH dictionary attack. The interesting results are obtained, as follows: (1) the several hosts generated the DNS query packet traffic, taking a rate of more than 1,000 hour^{-1}, through 07:30-08:30 in March 14th, 2009, (2) the DNS query packet traffic correlates with the DNS query packet one including more than two specific query keywords, and (3) the former keyword is a fully qualified domain name and the latter one is an IP address. Therefore, we can detect inbound SSH dictionary attack by watching frequencies of the FQDNs and the IP addresses as query keywords in the DNS query packets from the hosts in the campus network.
Keywords : Detection, SSH dictionary attack, DNS query traffic

1 Introduction

It is of considerable importance to raise up a detection rate of the SSH dictionary attack bots, since they become components of the bot clustered networks[1-3]. Unfortunately, the SSH dictionary attack has been still used to spread out the bots when hijacking the specific vulnerable network servers on the Internet. This is because the network servers can be easily connected with the SSH clients when the attackers know the user ID and its pass phrase, or when, in other words, the account holders use easy breakable pass phrases. Therefore, it is also important to develop detection technologies as countermeasures against the SSH dictionary attack[4].

In this paper, (1) we carried out statistical analysis on the total- A- and the PTR-resource records (RRs) based DNS query packet traffic from the SSH dictionary attacked Linux PC hosts through March 14th, 2009, and (2) we

assessed the detection rate of the SSH dictionary attack based DNS query traffic in the total DNS query packet traffic through January 1st to June 30th, 2009.

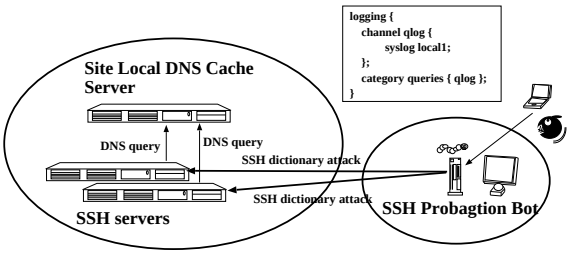

Figure 1. A schematic diagram of an observed network in the present study.

2 Observations

We investigated on the DNS query request packet traffic between the top domain (**tDNS**) DNS server and the network servers as DNS clients (Figure 1). The **tDNS** server is one of the top level domain name (kumamoto-u) system servers and plays an important role of domain name resolution including DNS cache function, and the operating system is Linux OS (CentOS 4.3 Final) in which the 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.

In the **tDNS** server, the BIND-9.2.6 program package has been employed as a DNS server daemon[5]. The DNS query packet and their query keywords have been captured and decoded by a query logging option (see Figure 1 and the named.conf manual of the BIND program in more detail). The log of DNS query packet access has been recorded in the syslog files. All of the syslog files are daily updated by the cron system. The line of syslog message consists of 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, or a mail exchange (MX RR) type.

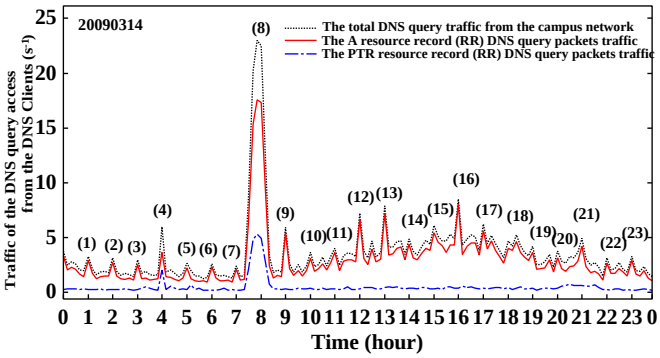

Figure 2. The total, A and PTR resource record based DNS query packet traffic between the top domain DNS (**tDNS**) server and the DNS client A at March 14th, 2009 (s^{-1} unit).

3 Results and Discussion

Firstly, we illustrate the observed total DNS query packet traffic, and A- and PTR-RRs based DNS query traffics from the campus network to the **tDNS** server in March 14th, 2009, as shown in Figure 2. In Figure 2, we can find twenty three peaks and they are categorized into two groups, as: {(1)-(3),(5)-(7),(9)-(23)} and {(4),(8)}. In the former group, the total DNS query packet

traffic correlates only with the A RR based DNS query packet traffic, while in the latter one, the total DNS query packet traffic does with the both A- and PTR-RRs based DNS query packet traffics.

We investigated statistics of the DNS query keywords in the total DNS query packet traffic in the peak (8) and the results are shown in Table 1. In Table 1, the top query keyword is a fully qualified domain name (FQDN) of the host on the Internet, and the second top one is an IP address corresponding to the FQDN. Interestingly, we investigated the syslog files in several network servers on the campus network, and then we observed the same FQDNs and the same IP addresses as the SSH clients on the Internet. We also found several signatures that the SSH clients tried repeatedly to login into the network servers in a short period *i.e.* this feature shows that the network servers were under SSH dictionary attack through 07:30 to 08:30 March 14th, 2009. Therefore, we can conclude that we can detect the SSH dictionary attack based DNS query packet traffic when the pairs of the top FQDNs and the IP addresses are observed in the top DNS query keywords (Table 1). To confirm this possibility, we illustrate calculated frequencies for the pairs of the FQDNs and the IP addresses as query keywords in the DNS query traffic from the campus network through January 1st, 2009, by configuring three threshold values of 1,000, 5,000, and 10,000 day^{-1}, shown in Figure 3.

Table 1. Detected top unique query keywords and their frequency in the total DNS query packet traffic from the university campus network through 07:30-08:30 March 14th, 2009. (hour^{-1} unit).

	DNS query keywords	Frequency (hour^{-1})
1	host*.t*.c*.*.net	31,604
2	7*.15.**.74	11,445
3	host*.t*.c*.*.net.kumamoto-u.ac.jp	1,551
4	host*.t*.c*.*.net.localdomain	1,046
5	host*.t*.c*.*.net.*.kumamoto-u.ac.jp	1,046

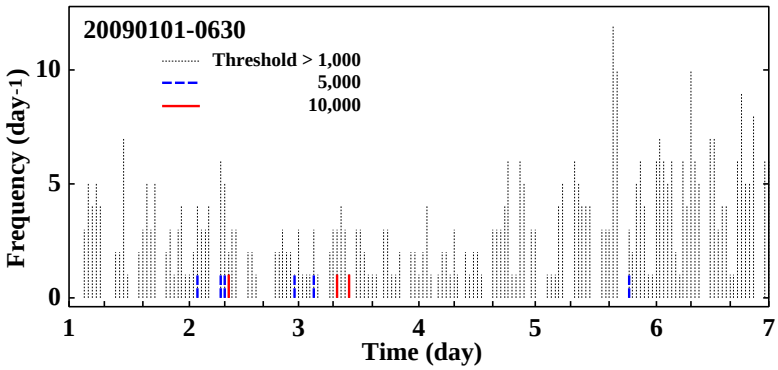

Figure 3. Frequency for the pairs of fully qualified domain names (FQDNs) and IP addresses as query keywords in the DNS query packet traffic from the campus network through January 1st to June 30th, 2009 (day^{-1} unit).

In Figure 3, we can observe a lot of peaks in a threshold value of 1,000 day^{-1}, however, these peaks can include much false positives, while in threshold values of 5,000 and 10,000 day^{-1}, we can observe not only several significant peaks, but they mean increase of false negatives.

4 Conclusions

We performed traffic analysis on the DNS query packet access from the campus network to the **tDNS** server through March 14th, 2009, when the campus network servers were under inbound SSH dictionary attack and we obtained the following results, as: (1) The A RR based DNS query packet traffic strongly correlates with the PTR RR based DNS query packet one, in 07:30-08:30, March 14th, 2009. (2) We can observe the specific pairs of the top FQDNs and IP addresses in the total DNS query packet traffic.

From these results, we can detect the SSH dictionary attack by only watching the DNS query packet traffic from the campus network servers.

Acknowledgements

This study is supported by the Grant aid of Graduate School Action Scheme for Internationalization of University Students (GRASIUS) No. 165240040213 in Kumamoto University.

References

[1] P. Barford and V. Yegneswaran: An Inside Look at Botnets, Special Workshop on Malware Detection, *Advances in Information Security*, Springer Verlag, 2006.

[2] J. Nazario: Defense and Detection Strategies against Internet Worms, I Edition; *Computer Security Series*, Artech House, 2004.

[3] J. Kristoff: Botnets, *North American Network Operators Group (NANOG32)*, Reston, Virginia (2004), http://www.nanog.org/mtg-0410/kristoff.html

[4] J. L. Thames, R. Abler, and D. Keeling: A distributed active response architecture for preventing SSH dictionary attacks, *Proceedings for the Southeastcon, 2008, IEEE*, Huntsville, AL, USA, 2008, pp. 84-89.

[5] BIND-9.2.6: http://www.isc.org/products/BIND/