International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Detection of NS Resource Record DNS Resolution Traffic, Host Search, and SSH Dictionary Attack Activities

Kazuya Takemori [1*] **Dennis Arturo Ludeña Romaña** [1*]

[1] *Graduation School of science and Technology, Kumamoto University,*
Kumamoto 860-8555, Japan

Shinichiro Kubota [2*] **Kenichi Sugitani** [2*] **and Yasuo Musashi** [2*]

[2] *Center for Multimedia and Information Technologies,*
Kumamoto 860-8555, Japan

[*] Corresponding author's Email:musashi@cc.kumamoto-u.ac.jp

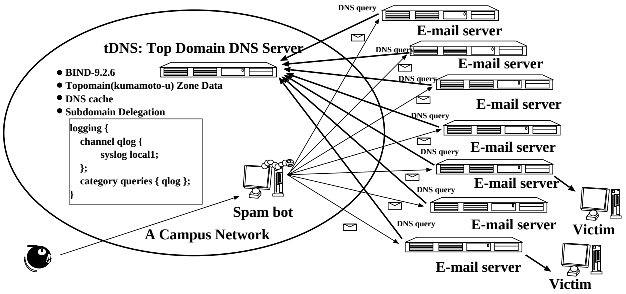
Abstract: We carried out an entropy study on the DNS query traffic from the Internet to the top domain DNS server in a university campus network through January 1st to March 31st, 2009. The obtained results are: (1) We observed a difference for the entropy changes among the total-, the A-, and the PTR resource records (RRs) based DNS query traffic from the Internet through January 17th to February 1st, 2009. (2) We found the large NS RR based DNS query traffic including only a keyword "." in the total inbound DNS query traffic. (3) We also found that the unique source IP address based PTR DNS traffic entropy slightly increased, while the unique DNS query keywords based one drastically decreased in March 9th, 2009. We found a specific IP host which was an already-hijacked classical Linux PC that carried out the SSH dictionary attack to the Internet sites in March 9th, 2009. From these results,we can detect the unusual inbound NS RR based DNS traffic and the outbound SSH dictionary attacks by only watching DNS query traffic from the Internet.

Keywords: DNS based detection, Dictionary Attack, DNS traffic entropy, Spam bots, Host search

1. Introduction

It is of considerable importance to raise up a detection rate of Bots, since they become components of the bot clustered networks that are used to transmit a lot of unsolicited mails including like spam, phishing, and mass mailing activities and to execute distributed denial of service attacks [1–4].

Wagner *et al.* reported that entropy based analysis was very useful for anomaly detection of the random IP search activity of Internet worms (IWs) like an W32/Blaster or an W32/Witty worm, respectively, since the both worms drastically changes entropy when after starting their activity [5].



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

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

Then, we reported previously that the unique DNS query keyword based entropy in the PTR resource record (RR) based DNS query packet traffic from the Internet decreases considerably while the unique source IP addresses based entropy increases when the random spam bots activity is high in the campus network [6]. This is probably because the PTR RR based DNS query packet traffic was generated by the spam bots activity sensors like a spam filter of the E-mail server and/or the intrusion detection/prevention system (IDS/IPS) on the Internet [6]. Therefore, we can detect spam bots activity, especially, a random spam bot (RSB) in the campus network, by watching the DNS query packet traffic from the other sites on the Internet (see Figure 1). We also reported that we observed not only an increase in the unique DNS query keyword based entropy in the PTR RR based DNS query packet traffic from the Internet but a decrease in the unique source IP address based one in the DNS query packet traffic when performing host search activity from the Internet [7].

In this paper, (1) we carried out entropy analysis on the total- A- and the PTR resource records (RRs) based DNS query packet traffic from the Internet through January 1st to March 31st, 2009, (2) we assessed the bot attack detection rate among the entropies for the total- A-RR, and the PTR-RR based DNS query packet traffic, and (3) we reported a new instance for detection of the random SSH dictionary attack [8].

2. Network Systems and DNS Query Packet Capturing

We investigated on the DNS query request packet traffic between the top domain (**tDNS**) DNS server and the DNS clients. Figure 1 shows an observed network system in the present study, which consists of the server and the PC clients as bots like a random spam bot and a host search one in the campus network, and the victim hosts like the E-mail servers on the Internet. 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 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 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 [9] has been employed as a DNS server daemon. 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 the contents 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, or a mail exchange (MX RR) type.

3. Estimation of Entropy

We employed Shannon's function in order to calculate entropy $H(X)$, as

$$H(X) = -\sum_{i \in X} P(i) \log_2 P(i) \qquad (1)$$

where X is the data set of the frequency $freq(j)$ of IP addresses or that of the DNS query keyword in the DNS query packet traffic from the outside of the campus network, and the probability $P(i)$ is defined, as

$$P(i) = \frac{freq(i)}{\sum_j freq(j)} \qquad (2)$$

where i and j $(i, j \in X)$ represent the unique source IP address or the unique DNS query keyword in the DNS query packet, and the frequency $freq(i)$ are estimated with the following script program:

```
#!/bin/tcsh -f
cat querylog | grep "client 133\.95\." | \
tr ’#’ ’ ’ | awk ’{print $7}’ | \
sort -r | uniq -c | sort -r >freq-sIPaddr
cat querylog | grep "client 133\.95\." | \
awk ’{print $9}’ | sort -r | uniq -c | \
sort -r >freq-keywords
```

Chart 1

where “querylog” is a syslog file including syslog messages of the BIND-9.2.6 DNS server daemon program [9]. The syslog message (one line) consists of keywords as “Month,” “Day,” “hours:minutes:seconds,” “server name,” “named[process identifier]:,” “client,” ”source IP address#source port address:,” “query:,” and “a DNS query keyword”. This script program consists of three program groups: (1) The first program group is a first line only including “#!/bin/tcsh -f” means that this script is a TENEX C Shell (tcsh) coded script programs. (2) The second program group estimates frequencies of the unique source IP addresses, consisting of of unix commands from “cat” to “sort -r” because the back slash “\” connects the line terminated by “\” with the next line in the tcsh program. In this program group, the “cat” shows all the syslog message-lines from the syslog file “querylog,” the "grep -v" command extracts only the message-lines excluding the source IP address of "133.95.x.y," the "tr" replaces a character '#' with a white space ' ', the unix command "awk '{print $7}"' extracts only a seventh keyword as "source IP address" in the message-line, the "sort -r | uniq -c | sort -r" commands sort the dataset of "source IP addresses" into the dataset of "unique source IP addresses" and estimate the frequencies of the unique source IP addresses and the final results are written into the file "freq-sIPaddr". (3) The last program group extracts the DNS query keywords from the syslog message-lines, sorts the dataset of "DNS query keywords" into the dataset of "unique DNS query keywords" and estimates the frequencies of the unique DNS query keywords. Finally, the results of the last program group are written the file into "freq-querykeywords". In the last program group, although almost the commands, arguments, and their options take the same as the second program group, the unix command "tr" and its arguments are removed and a new argument " '{print $9}' " replaces the arguments of the unix command "awk" in the second program group.

4. Attack Activity Models

We define three incidents detection models for random attack (RA) activity, targeted attack (TA) activity, and host search (HS) activity (See Figure 2), respectively.

A random attack (RA) activity model – since a random spam bot (RSB), a typical example for the RA activity model, randomly attacks various victim E-mail servers, the E-mail servers can try to check IP addresses and fully qualified domain names (FQDNs) for the RSB, with referring to the top domain DNS (**tDNS**) server in the campus network. This causes an increase in the number of the unique source IP addresses in the DNS query traffic but a decrease in the number of the unique DNS query keyword *i.e.* the unique source IP addresses- and the unique DNS query keyword-based entropies simultaneously increase and decrease, respectively, when the RA activity is high in the campus network.

A targeted attack (TA) activity model – since the targeted spam bot (TSB), for example, attacks a small number of specific victim E-mail servers in the campus network or on the Internet, the E-mail servers can check IP addresses and FQDNs for the TSB, with referring to the **tDNS** server in the campus network. This causes decreases in the unique IP addresses- and the DNS query keyword-based entropies when the TA activity is high.

A host search (HS) activity model – the host search activity can be mainly carried out by a small number of IP hosts on the Internet or in the campus network like bot compromised PCs. Since these IP hosts send a lot of the DNS reverse name resolution (the PTR RR based DNS query) request packets to the **tDNS** server, the unique IP addresses- and the unique DNS query-keywords based entropies decrease and increase, respectively.

It is very difficult find out the thresholds for detecting the above described anomaly activity. Here, we should also define thresholds for detecting these three kinds of malicious activity models, as setting to 1,000 packets day^{-1} for the frequencies of the top-ten unique source IP addresses or the DNS query keywords. The thresholds are arbitrarily defined but discussed in the previously reported paper [10] since the observation time window is one day and the entropy based detection model can be done by off-line.

Note that the thresholds are a specific value for the campus network and they strongly depend on a size or a capacity of the campus network so that we need to estimate thresholds when employing the suggested detection method. Furthermore, we should discuss on the thresholds corresponding to the dynamic DNS query traffic based detection technology in real time. Very recently, for instance, we have already reported to start developing the Euclidean distance based dynamic detection model for the host search (HS) activity [11].

5. Results and Discussion

5.1 Entropy Changes in Total- A- and PTR-RRs DNS Query Packet Traffic from the Internet

We demonstrate the calculated unique source IP address and unique DNS query keyword based entropies for the total-, A- and PTR-resource records (RRs) based DNS query request packet traffic from the Internet to the top domain DNS (**tDNS**) server through January 1st to March 31st, as shown in Figure 3.

In Figure 3A, we can find ten peaks and they are categorized into three groups, as: {(1), (7), (8), (10)}, {(2)-(6)}, and {(9)}. In the first peak group, all the peaks show a decrease in the unique source IP address based entropy and an increase in the unique DNS query keywords based one *i.e.* this feature indicates the host search (HS) activity. It is very important to detect the HS activity because the HS activity is mainly performed as preinvestigation on the campus net-

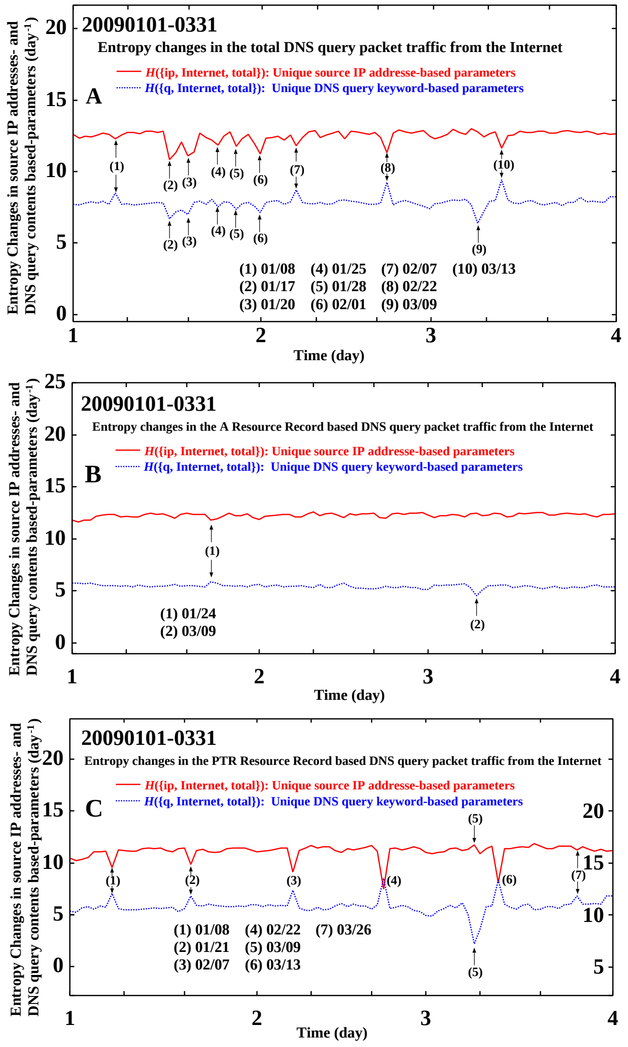


Figure 3. Entropy changes in the total-, A- and PTR-resource records (RRs) based DNS query request packet traffic from the campus network to the top domain DNS (**tDNS**) server through January 1st to March 31st, 2009. The solid and dotted lines show the unique source IP addresses and unique DNS query keywords based entropies, respectively (day^{-1} unit).

work for the next cyber attack. In the second group, we can observe the five peaks in which all the peaks demonstrate simultaneous decreases in the unique source IP address- and the unique DNS query keyword-based entropies. This feature shows that the peaks (2)-(6) can be assigned to a targeted attack (TA) activity mo-del. In the last group, we can find only a peak (9) which demonstrates nothing in the unique source IP addresses based entropy but a significant decrease in the unique DNS query keyword based one. This feature will be discussed later.

In Figure 3B, surprisingly, we can find only two peaks (1) and (2). In the peak (1), we can observe small increase and decrease in the unique source IP address- and the unique query keyword based entropies, respectively. The peak (1) can be assigned to January 24th, 2009. This is because we had a half-day hardware trouble in the campus network core switches at the day, and this fact could affect the entropy change. The peak (2) can be assigned to the same situation in the peak (9) in Figure 3A. As a result, we can observe no peak corresponding to the peaks for the targeted attack (TA) activity in Figure 3A.

In Figure 3C, we can find eight peaks which can be categorized into two groups, as: {(1)-(4), (6), (7)} and {(5)}. In the first group, we can observe the same peaks (1), (3), (4), and (6) corresponding to the peaks (1), (7), (8), and (10), respectively, in Figure 3A. This means that these peaks and the other peaks (2) and (7) can be allocated to the HS activity. Interestingly, in the peak (5), the unique source IP address based entropy increases in a slight manner, while the query keyword based entropy decreases significantly. This feature indicates a random attack (RA) activity model. Usually, however, we can observe clear symmetrical changes in the both entropies for the RA activity like a random spam bot (RSB) activity *i.e.* it has a possibility that the peak (5) demonstrates a different RA activity unlike a random spam bot (RSB) attack. Also, in Figure 3C, we can find out no TA activity peak like the peaks (2)-(6) in Figure 3A.

Therefore, we need to investigate further the total DNS query packet traffic at the TA activity peaks (2)-(6) in Figure 3A and to confirm the possibility showing a new instance for the RA activity at the peak (5) in Figure 3C.

5.2 The NS-RR DNS Query Packet Traffic from the Internet

We investigated statistics of the query keywords in the DNS query request packet traffic from the Internet at the peaks (2)-(6) in Figure 3A. The top query keywords was obtained when the frequency takes more than 1,000 packets day^{-1} and the FQDNs or IP addresses of the network servers are discarded, as listed in Table 1.

In Table 1, the top DNS query keyword is a root "." at each peak. Then, we performed DNS resource record (RR) based component analysis on the total DNS query packet traffic from the Internet including a root "." as the query keywords at the peaks (2) and (3) shown in Figure 3A. Usually, we can observe that the root "." included DNS query packet traffic takes only about 1,100 packets day^{-1} (an average through March 8th to 31st, 2009).

As shown in Table 2, the total root "." included DNS query packet traffic consists of the NS- and A-RRs

Table 1. Detected top/2nd unique query keywords and their frequency through January 17th to February 1st, 2009. (day^{-1} unit).

Peak	Date	Query keyword	Frequency (day^{-1})
(2)	Jan. 17th	.	69,927
		133.95.a1.181	1,473
(3)	Jan. 20th	.	72,291
		133.95.a1.181	1,619
		133.95.a2.55	1,384
(4)	Jan. 25th	.	40,419
(5)	Jan. 28th	.	51,810
		133.95.a1.181	1,523
(6)	Feb. 1st	.	47,690

Table 2. DNS resource record (RR) based component analysis on the total DNS query packet traffic from the Internet including a root "." as the query keywords at the two peaks, January 17th and 20th, 2009. (day^{-1} unit).

	Peak (2)	Peak (3)
	(Jan 17th, 2009)	(Jan 20th, 2009)
Total	69,927	72,291
A	274	162
AAAA	0	0
PTR	0	0
MX	0	0
TXT	0	0
NS	69,653	72,129
Others	0	0

Table 3. Detected top, 2nd, and third unique source IP addresses and their frequencies through January 17th to February 1st, 2009. (day^{-1} unit).

Peak	Date	Source IP address	Frequency (day^{-1})
(2)	Jan. 17th	69.50.a1.b1	44,002
		69.50.a2.b2	18,935
(3)	Jan. 20th	76.9.c1.d1	65,315
(4)	Jan. 25th	206.71.e1.f1	33,751
(5)	Jan. 28th	64.57.g1.h1	32,896
(6)	Feb. 1st	65.23.i1.j1	13,876
		71.6.k1.l1	13,875
		64.27.m1.n1	13,875

DNS query packet traffic in January 17th and 20th, 2009. Also, we can observe that the NS RR based DNS query traffic takes almost 1,300 packets day^{-1} (an average through March 8th to 31st, 2009).

We further obtained statistics of the source IP addresses in the root "." included DNS query packet traffic in January 17th and 20th, 2009, as shown in Table 3. We can see the specific IP addresses in Table 3, and these IP addresses can be assigned for targeted attack activity corresponding to the peaks (2)-(6) in Figure 3A.

5.3 A New Instance for the Random Attack Activity

We carried out statistics on the query keywords in the total PTR RR based DNS query packet traffic from the Internet at March 9th, 2009, in order to investigate further the peak (5) in Figure 3C. The results are shown in Table 4, in which the top IP addresses are obtained when the frequency takes more than or equal to 1,000 packets day^{-1}.

Table 4. Detected top, 2nd, and third unique query keywords and their frequencies through January 17th to February 1st, 2009. (day^{-1} unit).

	Query Keyword	Frequency (day^{-1})
1	133.95.s1.62	40,919
2	133.95.s2.73	6,110
3	133.95.s3.163	1,115

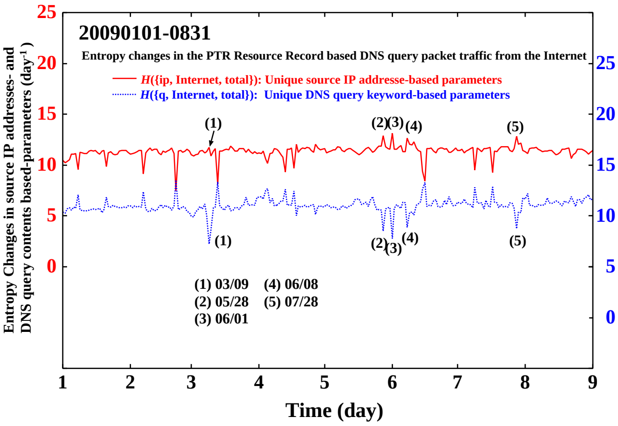


Figure 4. Entropy changes in the PTR-resource records (RRs) based DNS query request packet traffic from the campus network to the top domain DNS (**tDNS**) server through January 1st to August 31st, 2009. The solid and dotted lines show the unique source IP addresses and unique DNS query keywords based entropies, respectively (day^{-1} unit).

In Table 4, we can find the three top IP addresses of 133.95.s1.62, 133.95.s2.73, and 133.95.s3.163, in which the top IP address is assigned to the old Linux PC in the campus network. Fortunately, we received an automatic notifying E-mail in which they complained about that a PC terminal in the campus network had carried out the SSH dictionary attack to them and which shows the same IP address as the top one. Therefore, we can identify the peak (5) corresponding to the random SSH dictionary attack activity. Also, we calculated rate for the unique source IP address in the PTR RR based DNS query packet traffic including a query keyword "133.95.s1.62," in which the rate is calculated to be 11%.

Interestingly, the unique DNS query keyword based DNS traffic entropy considerably decreases while the unique source IP address based one increases slightly in the peak (5) in Figure 3C. This situation is different from the previous instances in the random attack (RA) activity like a random spam bot (RSB), since we previously reported that the both DNS traffic entropies

Table 5. Observed frequencies for the total source IP addresses and their unique source IP addresses of the PTR resource record (RR) based DNS query request packet traffic at March 9th, May 28th, June 1st and 8th, and July 28th, 2009 (day^{-1} unit).

Peak	Date	Frequency (day^{1})	
		Source IP Address	Unique Source IP Address
(1)	March 9th (SSHD)	40,919	4,317 (11%)
(2)	May 28th (RSB)	31,261	14,052 (45%)
(3)	June 1st (RSB)	44,575	20,474 (46%)
(4)	June 8th (RSB)	22,461	10,090 (45%)
(5)	July 28th (RSB)	34,748	16,066 (46%)

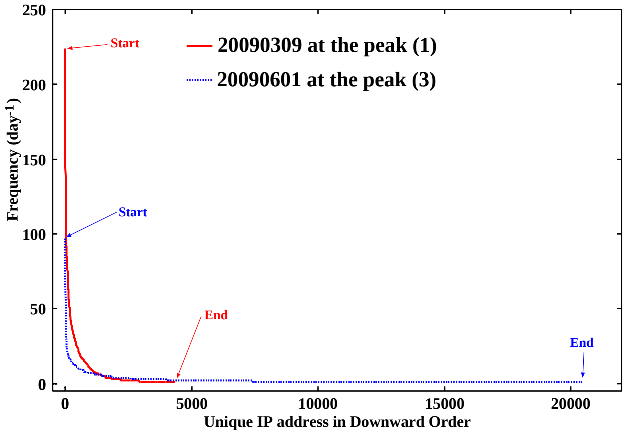


Figure 5. Frequency distribution in the unique source IP addresses of PTR-resource records (RRs) based DNS query request packet traffic from the Internet to the top domain name system (**tDNS**) server through March 9th and June 1st, 2009. The solid and dotted lines show the unique source IP addresses corresponding to the SSH dictionary attack (March 9th) and the random spam bot attack (June 1st) activities (day^{-1} unit).

change almost symmetrically in the peaks for the random spam bot activity [7, 12].

In May 28th, June 1st and 8th, and July 28th, 2009, we detected a random spam bot (RSB) in the campus network and we observed 31,261, 44,575, 22,461, and 34,748 packets day^{-1}, respectively, in which these days are corresponding to the peaks (2)-(5) showing in Figure 4. The rate for the unique source IP address were estimated to be 45-46% (see Table 5).

In Table 5, we can also notice that the source IP address based frequency takes a closest value at the peak (3). Thus, we compared the unique source IP address based frequencies between the peaks (1) and (3) in a downward ordered manner, and the results are shown in Figure 5, where the both peaks (1) and (3) are instances for the SSH dictionary attack and the random spam bot (RSB) attack activities, respectively.

In Figure 5, we can observe a short tail in the SSH dictionary attack based frequency distribution curve, while we can see a long tail in the RSB attack based one. Surely, the unique source IP address based entropies were calculated to be 10.72 and 13.63 for the peaks (1) and (3), respectively, *i.e.*

Table 6. The calculated N, K, L, $H(X)$, $Head$ and $Tail$ values for the SSH dictionary attack and the random spam bot (RSB) attack activities at March 9th and June 1st, 2009 (day^{-1} unit).

	N	*K*	*L*	*Head*	*Tail*	*H*(*X*)
SSH	4,317	2,186	2,131	9.69	1.03	10.72
RSB	20,434	3,980	16,494	6.88	6.75	13.63

$$H(\{\mathrm{uip}:\mathrm{SSH}\}) < H(\{\mathrm{uip}:\mathrm{RSB}\}). \qquad (3)$$

This difference can be interpreted in terms of a difference between the numbers for the SSH servers and the E-mail servers on the Internet.

In order to confirm this fact, we should calculate partial entropy values in the head and the tail in the frequency distribution curve. We define again eq 3 into the following eq 4, as

$$H(X) = Head + Tail \qquad (4)$$

where $Head$ and $Tail$ are defined as

$$Head = -\sum_{\mathrm{j=1}}^{\mathrm{K}} P(j) log_2 P(j) \qquad (5)$$

$$Tail = -\sum_{\mathrm{j=K+1}}^{\mathrm{L}} P(j) log_2 P(j) \qquad (6)$$

$$N = K + L \qquad (7)$$

where N means the unique source IP address number, K shows the number of unique source IP addresses which the frequency takes greater than 2 day^{-1}, and L represents the number of unique source IP addresses which the frequency takes less than or equal to 2 day^{-1}.

We show the calculated values for N, K, L, $H(X)$, $Head$ and $Tail$ in Table 6.

In Table 6, the N and L values for the SSH dictionary attack are significantly less than those for the RSB attack. Also, the $Tail$ value for the SSH dictionary attack is considerably less than that for the RSB attack. These features can contribute to the difference in the unique IP address based entropies for the SSH dictionary and the RSB attacks.

As a result, the difference in the entropies can be interpreted in terms that the E-mail servers are greater than the SSH ones on the Internet. This is probably because the SSH severs can be usually prohibited and permitted only the few specific users, while the E-mail servers should be widely opened to the unspecified servers and/or clients.

5.4 Related Works

Previously, we reported entropy study on the A and PTR resource records (RRs) based DNS query traffic from the Internet to the top domain name server (**tDNS**) through April 1st, 2007 to April 30th, 2008, in the paper [7], concluding that we can detect targeted a spam bot (TSB) and a random spam bot (RSB) in the A RR based DNS query traffic entropy and a RSB and a host search (HS) activity in the PTR RR based DNS query traffic one. Also, we can show a typical instance for the random spam bot (RSB) found in January 17th, 2008, the both unique source IP address and DNS query keyword based entropies change simultaneously and symmetrically.

In the present paper, (1) we can offer the newly found NS RR based DNS query request attack in the total DNS query traffic from the Internet to **tDNS**, in which the NS RR based DNS query request packets includes a "." as their payloads indicating that the attacker groups changed their strategy and tried their newly developed method to search the vulnerable DNS root servers, because the DNS servers answer the fully qualified domain names (FQDNs) and the IP addresses of the root DNS servers if the DNS servers receive the NS RR based DNS query request packet.

Furthermore, in this paper, (2) we can show the newly found SSH dictionary random attack based traces in the PTR RR based DNS query request traffic. In the random attack (RA) model like the random spam bot (RSB), the unique source IP address based entropy can change to a certain extent or in the almost same manner as the unique DNS query keyword based one. In the random SSH dictionary attack model, on the other hand, the unique source IP address based entropy changes a little, as compared with the unique DNS query keyword one [7]. This is because the SSH servers can be opened only to the specific supervisors for the IT systems in the organizations but the E-mail servers are more relatively and widely opened to the public users on the Internet *i.e.* this difference can be contributed to the small change of the unique source IP address based entropy in the PTR RR DNS query request traffic.

6. Conclusions

We investigated entropy analysis on the total, A, PTR, and NS resource record (RR) based DNS query request packet traffic from the Internet through January 1st to March 31st, 2009. The following interesting results are found: (1) we observed 10, 2, and 8 incidents in the entropy change in the total, A, and PTR based DNS query packet traffic, respectively. In the total DNS query packet traffic entropy change, we found 4 host search (HS) activities, 5 targeted attack (TA) ones, and 1 random attack (RA) one. In the A RR based DNS query packet traffic entropy change, we found 1 hardware trouble and 1 RA activity. In the PTR based DNS query packet traffic entropy change, we discovered 7 HS activities and 1 RA one. (2) We found that the specific IP hosts had carried out the TA attack to the campus top domain name server (**tDNS**) by transmitting the NS RR based DNS query packet traffic including a root "." as a query keyword. (3) Also, we found an instance for the RA activity like a random SSH dictionary attack but unlike a random spam bot (RSB). This is because we observed the difference in the source IP address based entropy change and the unique rates for the source IP address in the SSH dictionary and RSB attacks were calculated to be 11% and 45-46%, respectively.

We continue further study to develop detection technologies of spam and SSH dictionary attack bots.

Acknowledgments

All the studies were carried out in CMIT of Kumamoto University and 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] B. McCarty: "Botnets: Big and Bigger," *IEEE Security and Privacy*, No.1, 2003, pp. 87-90.

[5] A. Wagner and B. Plattner: Entropy Based Worm and Anomaly Detection in Fast IP Networks, In: *Proc. of the 14th IEEE Workshop on Enabling Technologies: Infrastracture for Collaborative Enterprises (WETICE 2005)*, Linköping, Sweden, 2005, pp.172-177.

[6] D. A. Ludeña Romaña, K. Sugitani, and Y. Musashi, "DNS Based Security Incidents Detection in Campus

Network," *International Journal of Intelligent Engineering and Systems*, Vol. 1, No.1, 2008, pp.17-21.

[7] D. A. Ludeña Romaña, S. Kubota, K. Sugitani, and Y. Musashi, "DNS Based Spam Bots Detection in a University," *International Journal of Intelligent Engineering and Systems*, Vol. 2, No.3, 2009, pp.11-18.

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

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

[10] D. A. Ludeña Romaña, H. Nagatomi, Y. Musashi, R. Matsuba, and K. Sugitani, "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, 2006, pp.39-46.
http://www.iwate-u.ac.jp/isic/ipc2006/jacn10/paper/-g01.pdf

[11] M. Lei, Y. Musashi, D. A. Ludeña Romaña, K. Takemori, S. Kubota, and K. Sugitani, "Detection of Host Search Activity in Domain Name Reverse Resolution Traffic," *IPSJ Symposium Series*, Vol. 2009, No.15, 2009, pp.91-94.

[12] D. A. Ludeña Romaña, S. Kubota, K. Sugitani, and Y. Musashi: DNS Based Spam Bots Detection in a University, In: *Proc. of the First International Conference on Intelligent Networks and Intelligent Systems (ICINIS2008)*, Wuhan, China, 2008, pp. 205-208.

[13] D. A. Ludeña Romaña, S. Kubota, K. Sugitani, and Y. Musashi, "Entropy Study on A and PTR Resource Record-Based DNS Query Traffic," *IPSJ Symposium Series*, Vol. 2008, No.13, 2008, pp.55-61.