Detection of Bot Worm-Infected PC Terminals

Dennis A. Ludeña Romaña,* Yasuo Musashi,** Ryuichi Matsuba,** and Kenichi Sugitani,**

**Graduate School of Science and Technology,*
Kumamoto University, Kumamoto-City, 860-8555, JAPAN
E-mail:dennis@st.cs.kumamoto-u.ac.jp

***Center for Multimedia and Information Technologies,*
Kumamoto University, Kumamoto-City, 860-8555, JAPAN
E-mail:musashi@cc.kumamoto-u.ac.jp

Abstract

The DNS query packet traffic in the topdomain DNS server for Kumamoto University were statistically investigated when infection of bot worm (BW) like W32/Mytob and W32/Zotob BWs were increased worldwidely. The interesting results are: (1) The W32/Mytob.A BW-infected PC terminal sends only the A resource record (RR) based DNS query packets including several keywords of “mail”, “smtp”, “mx”, “ns”, “gate”, and “relay” as their query contents. (2) The traffic of the abnormal client MX record based DNS query packet synchronizes with that of the abnormal random TCP access like ports of 135, 139, and/or 445 from the W32/Zotob BW-infected PC terminals. (3) The total traffic of the DNS query access from the outside of the campus network frequently correlates with that of the number of their unique source IP addresses. And (4) the unique source IP address-based entropy (randomness) also frequently correlates well with the query contents-based one. Thus, we can detect the IP addresses of the BW-infected PC terminals by watching the traffic of the DNS resolution access and the abnormal random TCP one.

Keywords: Bot Worm, Spam Bot, DNS-based Detection, Worm Detection, Entropy Analysis

1. Introduction

Recent internet worms becomes one of the big threats in the information- and communication-technology (ICT) based society. It is of considerable importance to raise up a detection rate of internet worms, especially, the bot worms (BWs), since the bot worm (BW) not only intrudes into the PC terminals but also hijacks the infected PC terminals [1-4]. After the infection or hijacking, the BW-infected PC terminal becomes usually a component (a bot) of the bot network system that is used to send a lot of unsolicited mails like spam, phishing, and mass mailing (a SMTP proxy), to carry out a distributed denial of service (DDoS) attack (a base for cyber attack), to launch new internet worms that infect with the next victim PC terminals (bot propagation like service attack worm (SAW) by illegal random IP address access to the TCP ports 135, 139, and/or 445), to spy out or disclosure a secret (information leakage/privacy disclosure), and so on [1]. From these points, it is required to develop a countermeasure method to detect the bot worm activity.

One of the conventional countermeasure methods is to detect client based MX (Mail Exchange) resource record (RR) DNS query access. We suppose that the client based MX RR DNS query access is suspicious because the usual PC terminals normally send only Address (A) resource record (RR) based DNS query packets [7-10]. This model is very useful to detect a mass mailing worm (MMW) like W32/Netsky and W32/Mydoom MMWs [11, 12] as well as the bot worm-infected victim PC terminals when transmitting spam mails. However, the recent bot worm (BW) like W32/Mytob and W32/Zotob BWs[13, 14] has been started to use the own remote DNS server (not a local DNS server) and/or to refrain the client based MX RR DNS query access so that it is hardly to find them. From this point, we need to develop several new countermeasure methods to detect the advanced bot worms.

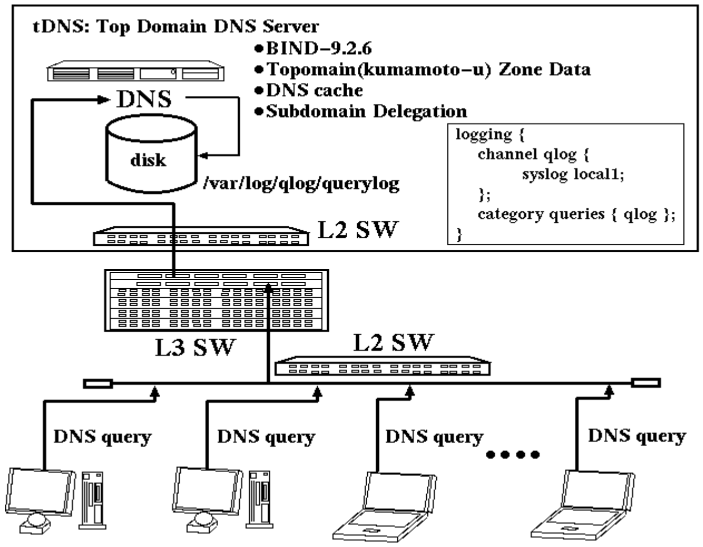
Recently, we observed abnormal A RR based DNS query traffic from the suspicious internet worm-infected PC terminal in the top domain name system (DNS) server Kumamoto University. This PC terminal was infected W32/Mytob.A bot worm (BW) [13]. In April 20th, 2005, on the other hand, we also observed strange but large scale DNS query traffic in a campus top domain DNS server (tDNS) like a denial-of-service (DoS) attack from the outside of the campus network. Unexpectedly, we failed to statistically find out the suspicious source IP addresses based DNS query traffic at the day. Initially, we considered that the abnormal DNS query traffic would be a large-scale IP address distributed DoS (DDoS) attack. And then we noticed that this big DNS query traffic is based on the DNS query packets traffic from the outside of the campus network, which were requested to perform name resolution on the specific IP addresses of E-mail servers and several PC terminals in the campus network.

The present paper is to discuss (1) on the abnormal A resource record (A RR) based DNS query access from the W32/Mytob.A BW-infected PC terminal at February, 25th, 2005, (2) the illegal TCP session trial access from the SAW-infected PC terminals, and the client MX RR based DNS query traffic through January 1st, 2005 to March 31st, 2006, (3) on correlation between the total DNS query packet traffic from the outside of the campus network and the frequency for the unique source IP addresses in the DNS query packets, (4) the entropy analysis of the frequencies of the unique source IP addresses and the DNS query contents, and (5) how to detect the BW worm-infected PC terminals (spam bots) in the campus network.

2. Observations

2.1 Network Systems

We investigated traffic of DNS query traffic between the top domain DNS server (**tDNS**) and the DNS clients. Figure 1 shows an observed network system in the present study and an optional configuration of the BIND-9.2.6 server program daemon [15] of the **tDNS**. The



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

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

tDNS[*] is one of the top level domain name (kumamoto-u) system servers and plays an important role of domain name resolution and subdomain delegation services for many PC terminals and the subdomain network servers, respectively, and the operating system is Linux OS in which the kernel-2.6.9 is currently employed with the 2GB core memory and 1Gbps EthernetPro Intel Network Interface Card.

2.2 Capture of DNS Query Packets

In **tDNS**, BIND-9.2.6 program package has been employed as a DNS server daemon [15]. The DNS query packets and their contents have been captured and decoded by a query logging option (Figure 1, or see % man named.conf). 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 resource record: A RR), an IP address (a PTR RR), and mail exchange (an MX RR).

2.3 Abnormal A RR based DNS Query Traffic from the PC terminal A

Firstly, we observed traffic of the A resource record (RR) based DNS query packets from the PC terminal A to the top domain DNS (**tDNS**) server through the day of February 25th, 2005 (Figure 2), because the PC terminal A is one of the top DNS query access clients in the day. In Figure 2, the traffic starts from 12:00 and ends after 17:30. We noticed this abnormal traffic 17:30 and we filtered this DNS query access. The numbers of the total DNS query packets, the A RR based DNS query packets, and the PTR RR based ones, are obtained to

[*] tDNS is a secondary top domain DNS server in Kumamoto University (kumamoto-u). The OS is Linux OS (kernel-2.6.9), and the hardware is an Intel Xeon 3.20GHz Two Dual Core SMP machine.

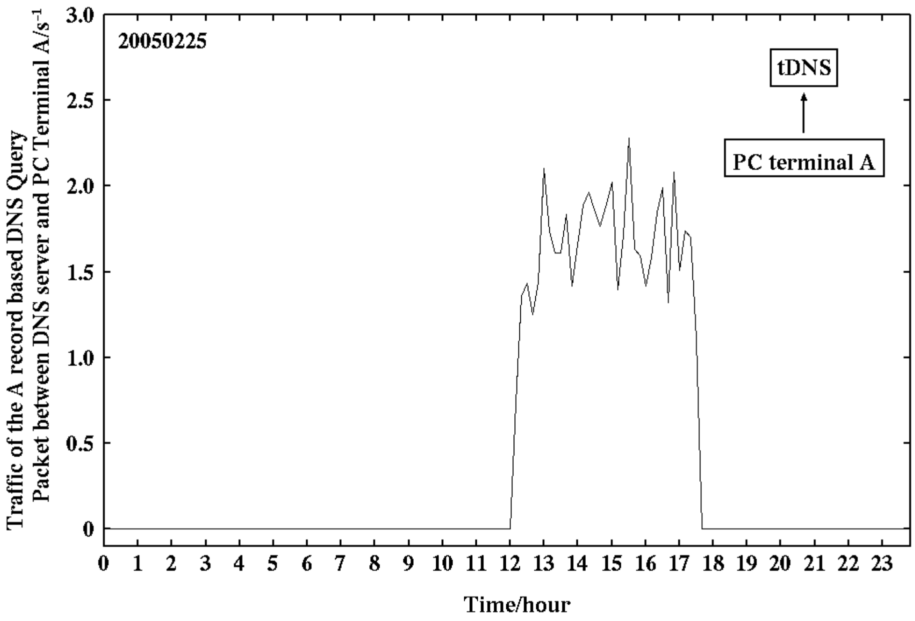


Figure 2. The the A resource record (RR) based DNS query traffic between the top domain DNS (**tDNS**) server and the PC terminal A at February 25th, 2005 (s^{-1} unit).

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 3. Statistics of the contents for the A resource record (RR) based DNS query packets from the PC terminal A at February 25th, 2005.

be 32,728/day, 32,721/day, and 7/day, respectively, and no MX RR based packet can be observed. This result shows that the total DNS query access traffic from the PC terminal A almost consists of the A RR based DNS query access traffic. We can demonstrate statistics of the query contents for the A RR based DNS query packets from the PC terminal A at February 25th, 2005 (Figure 3). In Figure 3, the keywords of “mail”, “smtp”, “mx”, “ns”, “gate”, and “relay” are used to generate fully qualified domain names (FQDNs) of the E-mail servers that have ever been observed when detecting IP addresses of the W32/Mydoom MMW-infected PC terminals [7], i.e. the PC terminal A is probably infected with a new type

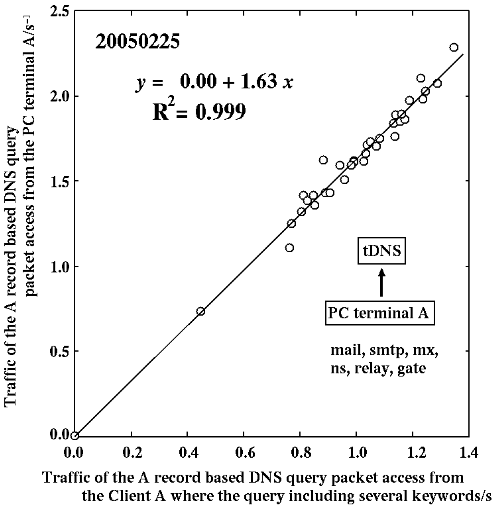


Figure 4. Total traffic of the A RR based DNS query packet access from the PC terminal A versus traffic of the A RR based DNS query packet access including the six keywords at February 25th, 2005

of mass mailing worm (MMW) which resembles well W32/Mydoom variants but it sends no MX RR based DNS query packet. 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 RR based DNS query packet access? This is probably because SMTP process needs the DNS solution twice: one is a mail exchange resolution (sending the MX RR based DNS query packet) to get an FQDN of the E-mail server and the other is standard resolution (sending the A RR based DNS query packet) to convert the FQDN into an IP address. In order to save the time for the former MX RR based name 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.

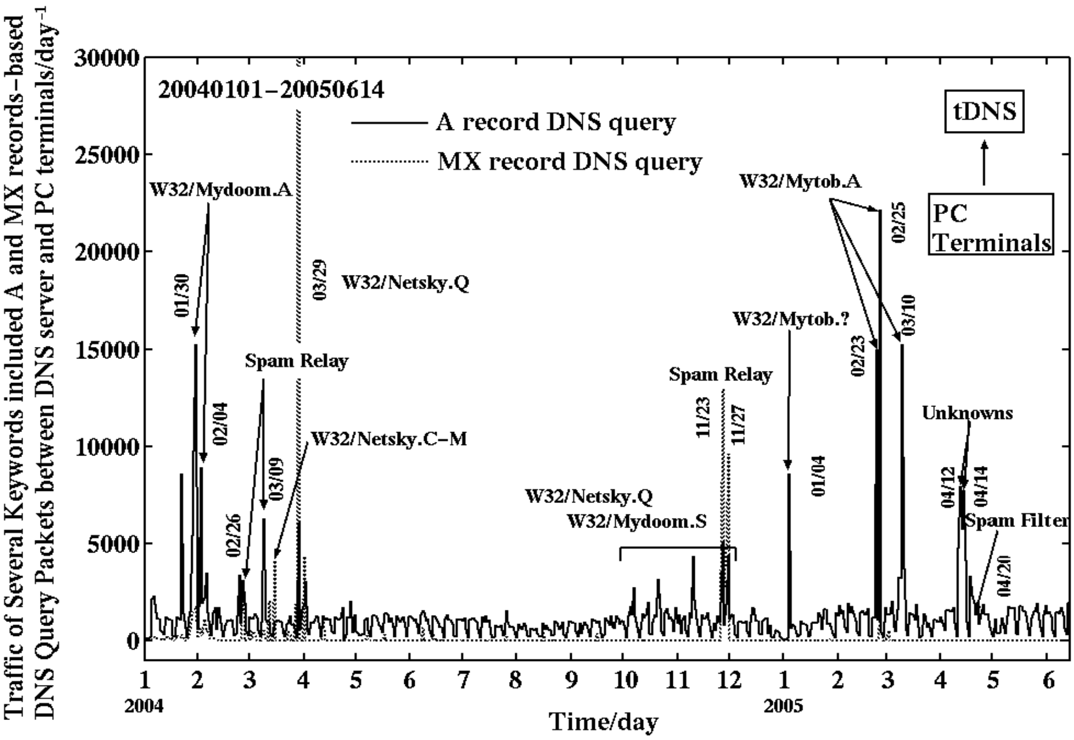


Figure 5. Total traffic of the A resource record (RR) based DNS query packet access including the six keywords (“mail”, “smtp”, “mx”, “ns”, “relay”, and “gate”) in the top domain DNS server (**tDNS**) through January 1st, 2004 to June 14th, 2005 (day^{-1} unit).

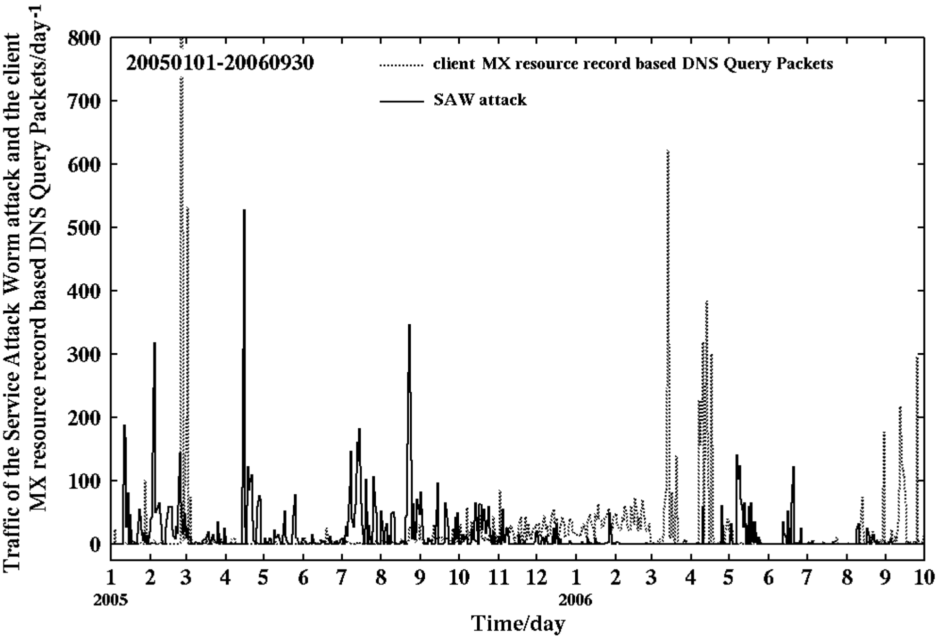


Figure 6. Traffic of the abnormal MX resource record (RR) DNS query packets and traffic of TCP session trial access from the service attack worm (SAW)-infected PC terminals through January 1st, 2005 to September 30th, 2006 (day^{-1} unit).

Figure 4 shows regression analysis on the total A RR based DNS query packet traffic from the PC terminal A versus the A RR based DNS query packet traffic from PC terminal A in which the six keywords of “mail”, “smtp”, “mx”, “ns”, “relay”, and “gate” are included. The data is February 25th, 2005. In Figure 4, the correlation coefficient (R2) is 0.999. This means that the traffic of the A RR based DNS query packet including the six keywords strongly correlates with the abnormal traffic of the A RR based DNS query packets from the PC terminal A. From this point, we have further investigated on the traffic of the A RR based DNS query packet access that includes several keywords consisting of head words in the FQDNs for E-mail servers.

We illustrate the observed total traffic of the A resource record (RR) based DNS query packet access including the six keywords (“mail”, “smtp”, “mx”, “ns”, “relay”, and “gate”) and the MX RR 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 5. 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.

2.4 W32/Zotob Bot Worm-infected PC terminals as a Spam Bot

The TCP session trial packets were recorded by the iplog-2.2.3 packet logger program package [16]. In Figure 6, we illustrate both traffic curves of the client MX resource record (RR) based DNS query packets and the TCP trial session access like the ports of 135, 139,

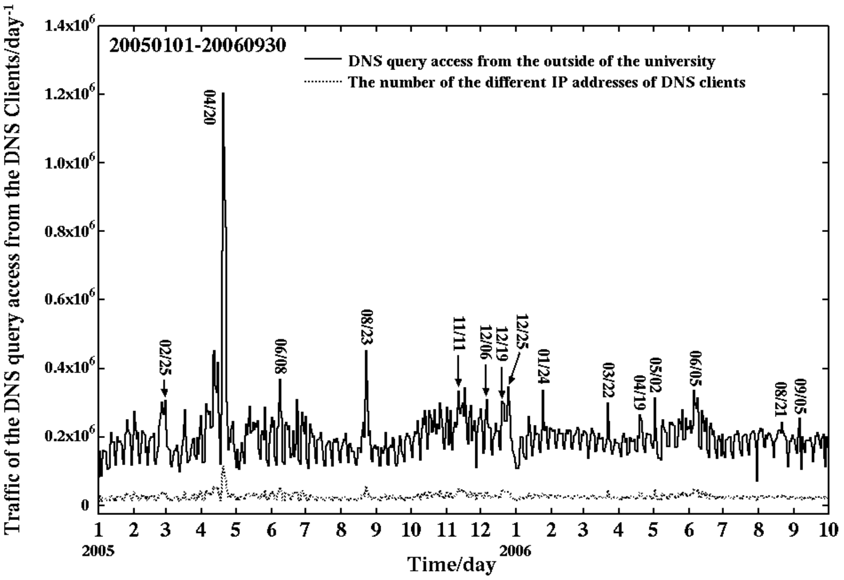


Figure 7. Traffic of the DNS query packets from the outside of the campus network to the top domain name system (**tDNS**) server through January 1st, 2005 to September 30th, 2006 (day^{-1} unit).

and 445 from the service attack worm (SAW)-infected PC terminals through January 1st, 2005 to September 30th, 2006. Interestingly, the both traffic curves start synchronizing after August 23rd, 2005 to February 27th, 2006. This feature shows that the BW like W32/Zotob variants transfer spam mails or mass mailing worms, since W32/Zotob variants were found after 13th August, 2005 [13]. However, the client MX RR based DNS traffic on the spam bots gradually decreases and the synchronization has been disappeared after the early days of March, 2006.

Therefore, we need hereafter the next new countermeasure method to detect these advanced bot worms (BWs).

2.5 The DNS query traffic from the outside of the Campus Network

We observed the total DNS query traffic from the outside of the campus network to the campus top domain DNS (**tDNS**) server through January 1st, 2005 to September 30th, 2006, as shown in Figure 7. In Figure 7, we can easily observe several peaks on the traffic curve at February 25th, April 20th, June 8th, August 23rd, November 11th, December 6th, 19th and 25th, 2005, January 24th, March 22nd, April 19th, May 2nd, June 5th, August 21st, and September 5th, 2006. Also, the traffic of the unique source IP address in the DNS query packets is shown in Figure 7. Interestingly, the both traffic curves synchronize each other at these peaks.

In April 20th, 2005, we observed most large-scale traffic for the **tDNS** and we reported that this large-scale traffic was generated by the spam filter of the E-mail servers in the internet [7a]. This is because the four keywords are shown in the DNS query packet traffic from the outside of the campus network, in which the four keywords consist of a fully qualified domain name (FQDN) of the **tDNS**, the subdomain local Email server, the two specific IP addresses of the subdomain local PC terminals. Furthermore, these four keywords were claiming on countermeasure against the E-mail spam bot in the campus network.

Thus, it can be significantly concluded that the abnormal DNS query traffic is caused by the spam filter on the E-mail server and/or the intrusion detection systems (IDSs) in the internet. Interestingly, the same situation has occurred after August 23rd, 2005, when infection of the W32/Zotob [14] variants was spreading worldwide. From these features, we can suppose that if the traffic of the unique source IP addresses in the DNS query packets access from the outside the campus network increases, this can provide us useful information to detect the campus related security incidents such as the bot worm (BW)-infected and/or hijacked PC terminals, the spamming E-mail server, and the base for cyber attack by only watching the DNS query traffic.

2.6 Estimation of Entropy

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

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

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

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

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

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

Chart 1

where "querylog" is a syslog file including syslog messages of the BIND-9.2.6 DNS server daemon program[15]. 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 “DNS query contents”. 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 and 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 contents from the syslog message-lines, sorts the dataset of “DNS query contents” into the dataset of “unique DNS query contents” and estimates the frequencies of the unique DNS query contents. Finally, the results of the last program group are written into the file “freqquerycontents”. 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.

3. Results and Discussion

3.1 Entropy Analysis in DNS Query Traffic

We illustrate the calculated entropy for the frequencies of the unique source IP addresses and the DNS query contents in the DNS traffic from the outside of the campus network to the top domain DNS (tDNS) server through January 1st, 2005 to September 30th, 2006, as shown in Figure 8.

In Figure 8, we can observe several significant peaks of (i) February 25th, (ii) April 20th, (iii) June 8th, (iv) August 23rd, (v) November 11th, (vi) December 6th, (vii) 19th and (viii) 25th, 2005, (ix) January 24th, (x) March 22nd, (xi) April 19th, (xii) May 2nd, (xiii) June 5th, (xiv) August 19th, and (xv) September 5th, 2006, and these peaks are the almost same as those in Figure 7.

Interestingly, in the peaks (i)-(xv), the unique source IP addresses-based entropy considerably increases, while the DNS query contents-based one significantly decreases.

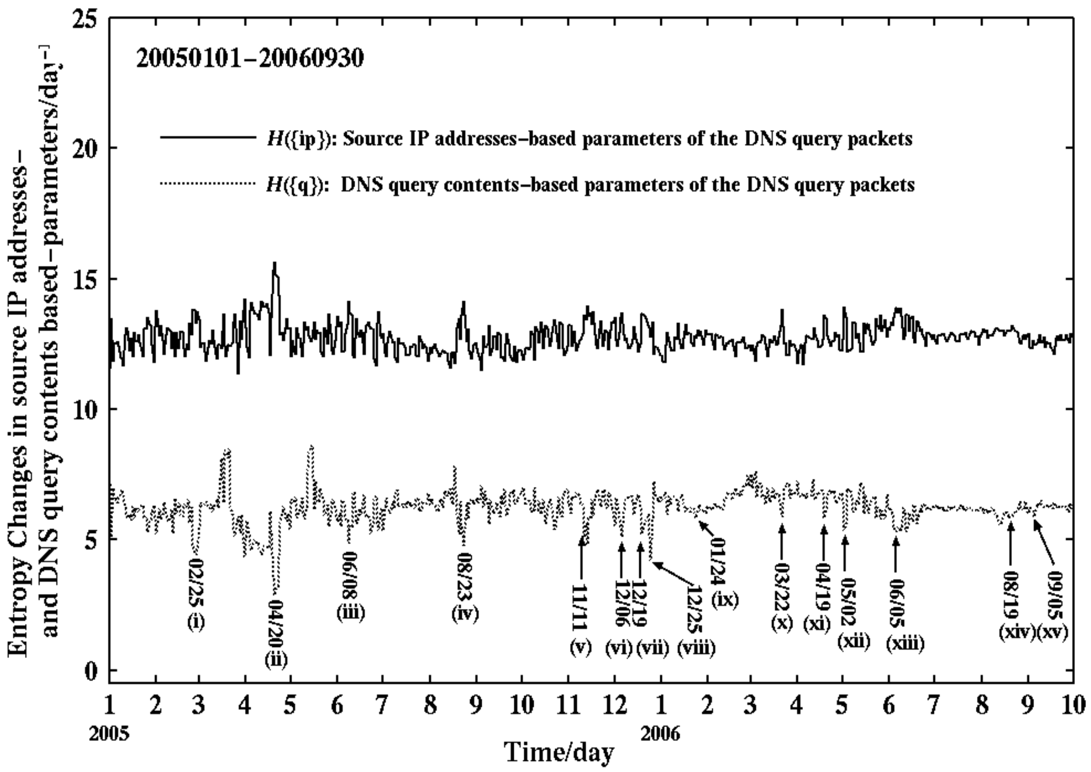


Figure 8. Entropy changes in the DNS query traffic from the outside of the campus network to the top domain name system (tDNS) server through January 1st, 2005 to June 30th, 2006 (day^{-1} unit).

These features show that if the DNS traffic from the outside of the campus network increases, it raises the degree of attention on the specific IP hosts like E-mail servers and/or PC terminals. And if the degree of attention increases, the query contents in the DNS query traffic will be concentrated several keywords i.e. the DNS query contents-based entropy drastically decreases [17].

In peak (i), the DNS query contents-based entropy decreases in the almost the same manner at peak (iv). This feature indicates that several local PC terminals are suspicious. It is fact that the several PC terminals were infected with the W32/Mytob.A bot worm (BW) at the day [13], and at the next day (February 26th, 2005), we received a lot of complaint E-mails from the outside of the university, in which we can find the local PC terminal IP addresses and these IP addresses are in agreement with the several top query contents in the DNS traffic from the outside of the campus network.

In other peaks (ii)-(xiii), we received a lot of similar complaint E-mails and the same IP addresses can be found at April 23rd, 2005 for the peak (ii), June 3rd for the peak (iii), August 23rd for peak (iv), November 26th for peak (v), December 5th for peak (vi), December 21st for peaks (vii) and (viii), January 27th, 2006 for peak (ix), March 22nd for peak (x), May 29th for peak (xii), June 9th, 16th, 22nd, and July 3rd for peak (xiii), and August 14th for peak (xiv).

Furthermore, we noticed that all the received complaint E-mails were related with the spam bot (spam mail sender/relay) in the campus network. This is because E-mail servers on the internet usually fight for detecting spam mails and they perform a lot of name resolutions on the source IP addresses of the spam senders (or spam bots). This feature probably generates an environment for increasing the degree of attention on the specific IP hosts in the campus network. On the other hand, we fortunately (unfortunately) received no complaint E-mail on a distributed denial of service (DDoS) attack, bot propagation like a service attack worms (SAWs), or information leakages. This fact indicates a possibility that method checking the degree of attention on the specific IP hosts cannot be used for detecting the bot worm (BW)-infected PC terminals based on the other BW functions like a DDoS attack, BW propagation, and/or information leakages in the present time.

This is probably because the spam bot function is carried out with the use of a lot of E-mail addresses so that the randomness for the spam bot function is probably much higher than those of the other BW functions. For instance, a cyber attack like a DDoS attack can be performed toward only several target sites and bot propagations are mainly act as a service attack worm (SAW) or a mass mailing worm (MMW) that can be easily detected by the local conventional intrusion detection system (IDS).

Note that in the present time, the BW-detection method by observing the degree of attention of the PC terminals in the campus network can be applied only for networks like campus networks or enterprise networks that consist of the inside LAN and the outside LAN (strictly). This feature shows that the BW-detection method seems to be difficult to implement it into the large-scale network class like an internet services provider (ISP).

As a result, it is clear that the decrease of the DNS query contents-based entropy means the increase of the degree of attention specific IP addresses and it can detect or identify the specific IP addresses as suspicious like bot worm (BW)-infected or hijacked PC terminals that mainly acts as a spam bot by only watching the several top query contents in the DNS traffic from the outside of the campus network.

3.2 Spam Bots in the Next Generation

Exceptionally, in the peaks (xi) and (xv) in Figure 8, the more than three suspicious IP addresses can be found, however, we did not received any complaint E-mail on them. This result means that we need a next countermeasure method since spam bots in the next generation surely use the local E-mail servers as a spam relay. We have continuously developed several detection systems against the spam bots so that conventional BWs can be easily found out by these detection systems and they need to change their conventional strategies like a direct transmission (SMTP) from the bots to targets. Probably, the next spam bots searches a vulnerable local E-mail server that can be easily accepted the local SMTP connection to the outside of the university.

For instance, a university local E-mail server had been crashed in the August 21st, 2006, because the E-mail server received a plenty of SMTP requests from the spam bots in the campus network so that the E-mail server failed into a situation such as lack of CPU and memory resources because of the mass SMTP connections. This incident indicates that spam bots change their methods to transfer the spam mails. Therefore, it can be said that we must continue further investigation to get more detailed information on the spam relay, especially, the local spam relay, in order to develop a new countermeasure technology against the spam bots in the next generation.

4. Concluding Remarks

We investigate statistically the DNS traffic between the top domain DNS server (**tDNS**) and the DNS clients. It can be concluded that the A resource record (RR) based DNS query packet access from the W32/Mytob BWs-infected PC terminals includes the six keywords and the traffics of abnormal client based MX RR type DNS query packets and TCP session trial access from the W32/Ztob BWs-infected PC terminals synchronizes each other. These results indicate that we can detect bot worms (BWs) by watching the synchronization in traffics of the PC terminal A and MX RRs based DNS query packets and TCP session trial like port 135, 139, and 445, like service attack worms (SAW).

Also, we carried out statistical investigation on the DNS query traffic from the outside of the campus network to the **tDNS** server to search the traces of security incidents, especially bot worm (BW)-infected PC terminals as spam bots in the campus network. The total DNS query traffic frequently correlates well with that of the unique source IP addresses in the campus network. The entropy based on the frequency of the DNS query contents in the DNS query traffic decreases when the entropy based on the frequency of the source IP addresses increases. From these results, it can be clearly concluded that we can detect the security incidents, especially bot worm (BW)-infected PC terminals as spam bots on the campus network by only watching the DNS query traffic from the other sites on the internet.

We further continue to develop detection and prevention systems based on the results of the present paper and to evaluate of detection of the bot worm (BW)-infected PC terminals as spam bots in the university because the results show that the newly developed countermeasure method detects the BW-related incidents in a considerably precise manner. However, very recent spam bots, in the next generation, probably, they would use the local E-mail servers as a spam relay. Conventionally, the spam relay is mainly used by the third party relay, for instance, like the third party uses the E-mail servers in the other sites. We have developed several detection systems against spam bots so that conventional BWs can be easily found out by these detection systems and they will change their strategies not to transmit spam mails directly, while to send spam ones, indirectly, probably via the local E-mail servers. From this point, we have already started again to develop a new countermeasure technology like watching the DNS query traffic from the E-mail server.

Acknowledgement All the calculations and investigations were carried out in Center for Multimedia and Information Technologies (CMIT), Kumamoto University. We gratefully thank to all the CMIT staffs and system engineers of MQS (Kumamoto) for daily supports and constructive cooperation.

References

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

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

[3] (a) Kristoff, J., Botnets, detection and mitigation: DNS-based techniques, *Northwestern Univerisity*, 2005, http://www.it.northwestern.edu/bin/docs/bots_kristoff_jul05.ppt. (b) Kristoff, J., Botnets, *North American Network Operators Group (NANOG32)*, Reston, Virginia (2004), http://www.nanog.org/mtg-0410/kristoff.html

[4] David, D., Zou, C., and Lee, W., Model Botnet Propagation Using Time Zones, *Proceeding of the Network and Distributed System Security (NDSS) Symposium 2006*; http://www.isc.org/isoc/conferences/ndss/06/proceedings/html/2006/

[5] Schonewille, A. and v. Helmond, D. –J., The Domain Name Service as an IDS. How DNS can be used for detecting and monitoring badware in a network, 2006; http://staff.sciece.uva.nl/~delaat/snb-2006/p12/report.pdf

[6] McCarty, B.: Botnets: Big and Bigger, *IEEE Security and Privacy*, No.1, pp.87-90 (2003).

[7] (a) Musashi, Y., Matsuba, R., and Sugitani, K., Detection, Prevention, and Managements of Security Incidents in a DNS Server, *Proceeding for the 4th International Conference on Emerging e-learning Technologies and Applications (ICETA2005)*, Košice, Slovakia, 2005, pp.207-211. (b) Musashi, Y., Matsuba, R., and Sugitani, K., Indirect Detection of Mass Mailing Worm-Infected PC Terminals for Learners, *Proceeding for the 4th International Conference on Emerging Telecommunications Technologies and Applications (ICETA2004)*, Košice, Slovakia, 2004, pp.233-237.

[8] (a) Musashi, Y., Matsuba, R., and Sugitani K.: Prevention of A-record based DNS Query Packets Distributed Denial-of-Service Attack by Protocol Anomaly Detection, *IPSJ SIG*

Technical Reports, Distributed System and Management 38th (DSM38), Vol. 2005, No.83, pp.23-28 (2005). (b) Matsuba, R., Musashi, Y., and Sugitani K.: Detection of Mass Mailing Worm-infected IP address by Analysis of Syslog for DNS Server, *IPSJ SIG Technical Reports, Distributed System and Management 32nd (DSM32)*, Vol. 2004, No.37, pp.67-72 (2004).

[9] Whyte, D., van Oorschot, P. C., and Kranakis, E., Addressing Malicious SMTP-based Mass-Mailing Activity Within an Enterprise Network, *Carleton University, School of Computer Science, Technical Report TR-05-06.pdf* (May 2005). http://www.scs.carleton.ca/research/tech_reports/2005/download/TR-05-06.pdf

[10] Ishibashi, K., Toyono, T., Toyama, K., Ishino, M., Oshima, H., and Mizukoshi, I., Detecting Mass-Mailing Worm infected Hosts by Mining DNS Traffic Data, *Proceeding of the 2005 ACM SIGCOMM workshop on Mining network data*, Philadelphia, Pennsylvania, USA, 2005, pp.159-164.

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

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

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

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

[15] http://ww.isc.org/products/BIND/

[16] http://ojnk.sourceforge.net/

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