A DNS-based Countermeasure Technology for Bot Worm-infected PC terminals in the Campus Network

Dennis A. Ludeña Romaña,[†] and Hirofumi Nagatomi[†]

[†]*Graduate School of Science and Technology, Kumamoto University,*
Kumamoto 860-8555 Japan,
E-mail: {dennis,nagatomi}@st.cs.kumamoto-u.ac.jp

Yasuo Musashi,[‡] Ryuichi Matsuba,[‡] and Kenichi Sugitani[‡]

[‡]*Center for Multimedia and Information Technologies, Kumamoto University,*
Kumamoto 860-8555 Japan,
E-mail: {musashi,matsuba,sugitani}@cc.kumamoto-u.ac.jp

Abstract: The DNS query traffic in a campus top domain DNS server were statistically investigated in order to find out the security incidents, especially bot worm (BW)-infected PCs on the campus network. The interesting results are obtained: (1) 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. (2) The unique source IP address-based entropy (randomness) also frequently correlates well with the query contents-based one. Therefore, these results indicate that we can detect suspicious IP hosts, especially, spam bots in the campus network by only watching DNS query traffic from the outside of the university.

Keywords: Bot worm, DNS-based detection, worm detection, entropy analysis, spam bot

1. Introduction

It is of considerable importance to raise up a detection rate of internet worms, especially bot worms (BWs), since the bot worm (BW) not only intrudes into the PC but also hijacks the infected PCs[1-4]. After the infection or hijacking, the BW-infected PC becomes usually a component of the bot network (a bot) that are 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 PCs (bot propagation), to spy out or disclosure a secret (information leakage), and so on[1]. From these points, it is required to develop a countermeasure method to detect the bot worm action.

One of the conventional countermeasure methods is to detect client based MX (Mail Exchange) resource record (RR) access. We suppose that the client based MX RR access is suspicious because the usual PC clients 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 PCs 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 or suppress the client based MX RR access so that it is hardly to find them. From this point, we need to develop a new countermeasure method to detected the advanced bot worms.

In April 20th, 2005, we 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 the campus network, which were requested to perform name

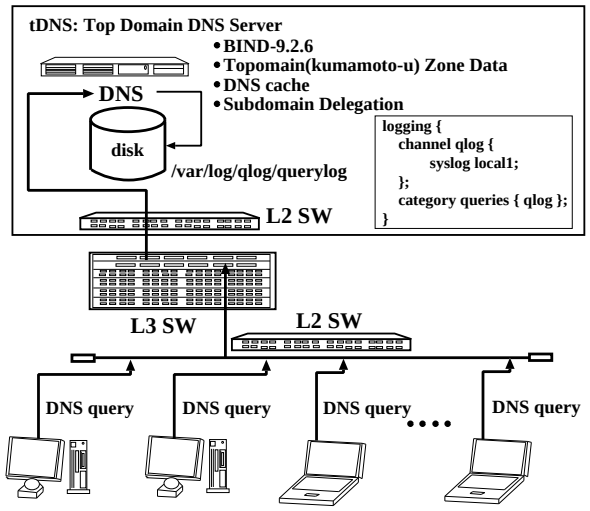

Figure 1. A schematic diagram of a network observed in the present study.

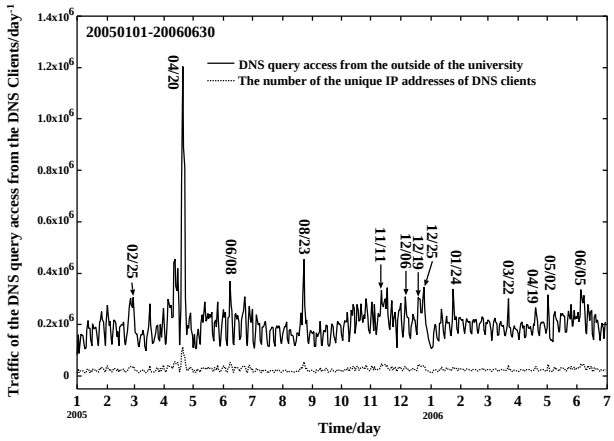

Figure 2. Traffic of the DNS query packets from the outside of the campus network to the top domain name system (**tDNS**) server through January 1st, 2005 to June 30th, 2006 (day^{-1} unit). The solid line shows total DNS query traffic and the dotted line indicates the number of the unique source IP addresses.

resolution on the specific IP addresses of E-mail servers and several PCs.

The present paper is to discuss (1) 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, (2) the entropy analysis of the frequencies of the unique source IP addresses and the DNS query contents, and (3) how to detect the BW worm-infected PCs (spam bots) in the campus network.

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 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 **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 PCs and the subdomain network servers, respectively, and the operating system is Linux OS in which the kernel-2.4.32 is currently employed with the 1GB core memory and 100Mbps 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 The DNS query traffic from the outside of the Campus Network

Firstly, 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 June 30th, 2006, as shown in Figure 2. In Figure 2, 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, and June 5th, 2006. Also, the traffic of the unique source IP address in the DNS query packets is shown in Figure 2. 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 E-mail server, the two specific IP addresses of the subdomain local PCs. Furthermore, these four keywords

were included in the received complaint mails claiming on countermeasure against the E-mail spam bot in the campus network.

Therefore, 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 PCs, the spamming E-mail server, and the base for cyber attack by only watching the DNS query traffic.

2.4 Estimation of Entropy

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

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

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

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

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 "freq-querycontents". 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 June 30th, 2006, as shown in Figure 3.

In Figure 3, 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,

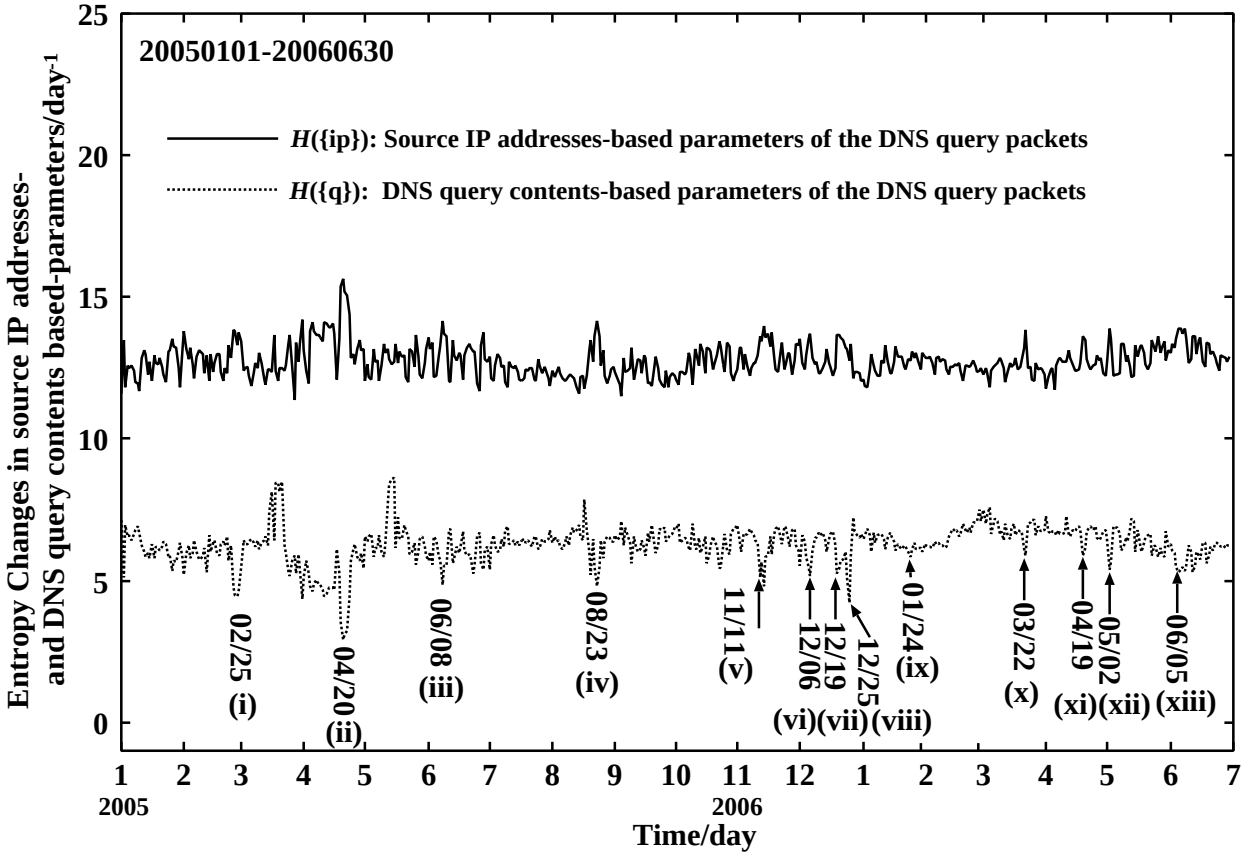

Figure 3. Entropy changes in the DNS query traffic from the outside of the campus network to the top domain name system (**tDNS**) server through January 1st, 2005 to June 30th, 2006 (day^{-1} unit). The both solid and dotted lines show entropies based on the data set of the number of the unique source IP addresses and on the frequency of the unique DNS query contents, respectively.

(vii) 19th and (viii) 25th, 2005, (ix) January 24th, (x) March 22nd, (xi) April 19th, (xii) May 2nd, and (xiii) June 5th, 2006, and these peaks are the same as those in Figure 2.

Interestingly, in the peaks (i)-(xiii), the unique source IP addresses-based entropy considerably increases, while the DNS query contents-based one significantly decreases. 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 PCs. 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[16].

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 PCs are suspicious. It is fact that the several PCs were infected with the W32/Mytob 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 client 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, 2005 for the peak (iii), August 23rd, 2005 for peak (iv), November 26th, 2005 for peak (v), December 5th, 2005 for peak (vi), December 21st. 2005 for peaks (vii) and (viii), January 27th, 2006 for peak (ix), March 22nd, 2006 for peak (x), May 29th, 2006 for peak (xii), June 9th, 16th, 22nd, and July 3rd for peak (xiii). Exceptionally, in the peak (xi), the three suspicious IP addresses can be found, however, we did not received any complaint E-mail.

Furthermore, we noticed that all the received complaint E-mails were related with the spam bot (spam E-mail sender) 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 PCs based on the other BW functions like a DDoS attack, BW propagation, and/or information leakages.

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 PCs 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 PCs 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 A New Countermeasure Method Against Bot Worm

In order to develop a countermeasure method, we define here detection as whether or not the frequency of an IP address or a fully qualified domain name (FQDN) exceeds a threshold. The detection rate is defined as the number of the detected IP addresses or FQDNs. In other words, we performed here statistics on the query contents of the DNS query packet traffic from the outside of the campus network.

To estimate the detection rate, we scanned the top DNS query contents in the DNS query traffic from the outside of the campus network to the top domain DNS (**tDNS**) server with three thresholds of 1000 day^{-1} (candidate), 5000 day^{-1} (warning), and 10000 day^{-1} (emergency), respectively, through January 1st, 2005

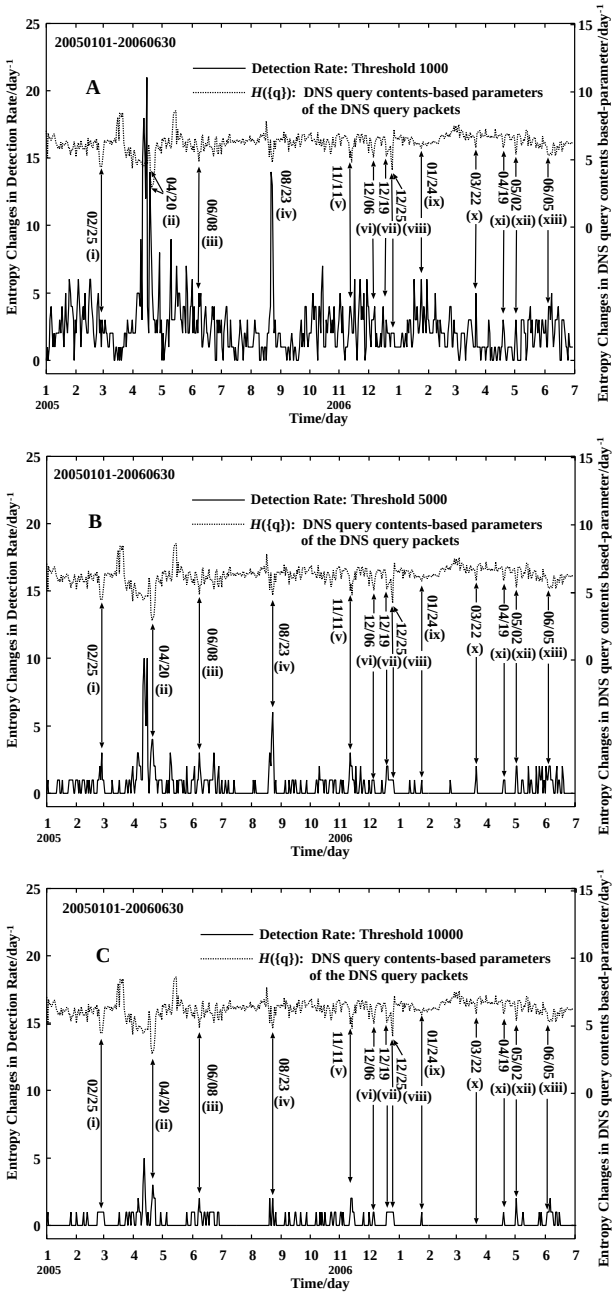

Figure 4. The estimated detection rate of the bot worm-infected PCs (the solid line)and the entropy changes based on the frequency of the unique DNS query contents (the dotted line) through January 1st, 2005 to June 30th, 2006 (day^{-1} unit).

to June 30th, 2006 (Figure 4) in which the thresholds are experimentally estimated, as follows: We investigated several top frequencies of the query contents in the DNS query traffic from the outside of the campus network at the days of peak (i)-(xiii) in Figure 3. We noticed that several frequencies take more than 10000 day^{-1} and the other frequencies estimated to be more than 1000 day^{-1} but less than 10000 day^{-1}. The suspicious IP addresses or FQDNs taking more than a frequency of 10000 day^{-1} were surely pointed out in the almost complaint E-mails. Thus, we can employ a frequency value of 10000 day^{-1} as a threshold for "emergency" or critical situation. Also, the

suspicious IP addresses or FQDNs corresponding to frequencies through 1000-10000 day^{-1} were found in the several complaint E-mails so that we can determine arbitrarily two kinds of thresholds like frequencies value of 1000 and 5000 day^{-1} for "candidate" and "warning" situations, respectively, because we cannot overlook the possibilities for existing of the bot worm (BW)-infected PCs in these frequencies taking through 1000-5000 day^{-1}. Note that the thresholds are a specific value for the campus network and they probably depend on a size of the campus network (We need to estimate thresholds when employing this detection method).

In Figure 4A (Threshold: 1000), the detection rate curve looks to be noisy and obscure. Surely, the detection rate takes not only high values in appearance but also produces much false positive. However, we can easily get much information on IP addresses or fully qualified domain names (FQDNs) of the suspicious candidate PCs in the campus network by checking the detection rate in this threshold (1000). Interestingly, the top and second largest peaks are located at April 15th and 12th, 2005, and their detection rate are estimated to be 21 and 18 day^{-1}. On the other hand, the detection rate of April 20th, 2005, is only 7 day^{-1}. In fact that at April 12th, several PCs in the campus network were infected with W32/Mytob variant bot worms (BWs) which transmit illegal A RR based DNS query packets including direct IP addresses as their query contents[8a]. This feature also indicates that it is useful to take the statistics of the query contents in the DNS query packet traffic from the outside of the campus network.

In Figure 4B (Threshold: 5000), the curve looks to be milder but more clear than that in Figure 4A. In this threshold, we should provide information on the detected IP addresses or FQDNs to the users and their managers to cope with the incident. The notification should be carried out automatically.

In Figure 4C (Threshold: 10000), the detection rate is a little bit quiet but the frequencies of the detected IP addresses or FQDNs in the threshold should be filtered quickly as possible and this fact should be notified to the users or their managers

As a result, it is clear that (1) the detection rate depends on the threshold, (2) we carefully treat the detection results of this countermeasure method, and (3) the countermeasure method is simply represented as a script as follows:

```
#!/bin/tcsh -f
cat freq-querycontents | th 1000  >candidate
cat freq-querycontents | th 5000  >warning
cat freq-querycontents | th 10000 |\
awk '{print $2}' >filter
cat warning | mail manager@gehogeho.org
cat filter | mail manager@gehogeho.org
foreach i($filter)
  iptables -A INPUT -s $i -j DROP
end
```

Chart 2

where the file "freq-querycontents" has been created by the script program in Chart 1, in which the line of the file consists of "frequency" and "the unique DNS query contents (IP addresses or fully qualified domain names)". This script program consists of three program groups: (1) The first program group (the 1st line) is as the same as that in Chart 1. (2) The second program group (the 2nd-7th lines) scans frequencies of the DNS query contents with the three kinds of thresholds of 1000, 5000, and 10000, and their scanned results are written into the files, "candidate", "warning", and "filter", respectively. The "`th`" command is a program that reads a line with the format (`''%15d%50s'', &threshold, &querycontents`) and if the value of the `threshold` variable takes more than the value of the first argument variable (`argv[1]`), print out the read line into the standard output. The IP addresses or fully qualified domain names in the files "warning" and "filter" are automatically E-mailed to the local PC- or network-managers. (3) The third program group (the 8th-10th lines) filters the IP addresses listed in the file "filter" and employs here, for example, the iptables in the Linux OS, to execute the source IP address based packet filtering.

4. Concluding Remarks

We investigated statistically on the DNS query traffic from the outside of the campus network to the top domain DNS (**tDNS**) server to search the traces of security incidents, especially bot worm (BW)-infected PCs 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 PCs as spam bots on the campus network by only

watching the DNS query traffic from the other sites on the internet.

We 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 PCs 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.

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 cooperations.

References and Notes

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

[3] (a) Kristoff, J., Botnets, detection and mitigation: DNS-based techniques, *Northwestern University*, 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.isoc.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.science.uva.nl/~delaat/snb-2005-2006/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 3rd 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* (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., Ohshima, 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://www.isc.org/products/BIND/

[16] Wagner, A. and Plattner, B., Entropy Based Worm and Anomaly Detection in Fast IP Networks, *Proceedings of 14th IEEE Workshop on Enabling Technologies: Infrastracture for Collaborative Enterprises (WETICE 2006)*, Linköping, Sweden, 2005, pp.172-177