INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Evaluation of DNS Based SSH Dictionary Attack Traffic in Campus Network

Masaya Kumagai[1], **Yasuo Musashi**[2*], **Dennis Arturo Ludeña Romaña**[1]

[1] *Graduate School of Science and Technology, Kumamoto University,*
2-39-1 Kurokami, Kumamoto, JAPAN, 860-8555
[2] *Center for Multimedia and Information Technologies, Kumamoto University,*
2-39-1 Kurokami, Kumamoto, JAPAN, 860-8555

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

Abstract: We performed statistical analysis on the total PTR resource record (RR) based DNS query packet traffic from a university campus network to the top domain DNS server through March 14th, 2009, when the network servers in the campus network were under inbound SSH dictionary attack. The interesting results are obtained, as follows: (1) the network servers, especially those providing SSH services, generated the significant PTR RR based DNS query request packet traffic through 07:30-08:30 in March 14th, 2009, (2) we calculated sample variance for the DNS query request packet traffic, (3) the variance can change in a sharp manner through 07:30-08:30, (4) we developed a couple of DNS based SSH detection technologies by employing the PTR RR DNS query request packet traffic variance- and the DNS query keywords Euclid distance based methods, and (5) we evaluated and compared the both detection rates. As a result, although the both detection technologies take high detection rates, the Euclid distance based detection technology can take a low false positive rate than that of the variance based one, indicating that we can detect the inbound SSH dictionary attack to the network server in the campus network by observing the total PTR RR DNS query request packet traffic from the campus network.

Keywords: DNS based Detection; SSH dictionary attack; SSH brute force attack; Euclid distance; variance

1. Introduction

It is of considerable importance to increase the detection rate of SSH dictionary attacks. Currently, most of SSH dictionary attacks are gererated from the attack bots, and if the SSH dictionary attack succeeds, the bots upload Trojan software to the SSH server and converts it into an attack bot too [1-4]. Unfortunately, the SSH dictionary attack (the brute force attack) has been still used to spread out the bots when hijacking the specific vulnerable network servers on the Internet [5, 6]. This is because the network servers can be easily connected with the SSH clients when the attackers know their user IDs and pass phrases, or when, in other words, the account holders use easy breakable pass phrases. Therefore, it is also important to develop

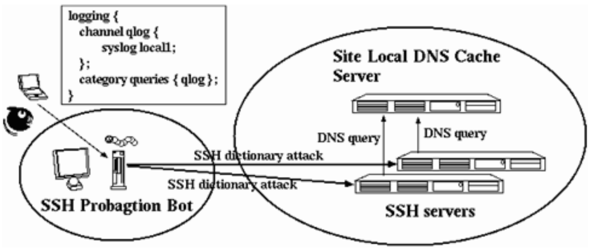

```
logging {
  channel qlog {
      syslog local1;
  };
  category queries { qlog };
}
```

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

detectiontechnologies as countermeasures against the SSH dictionary attack [5, 6].

Recently, several researchers reported prevention technologies for the SSH dictionary attack by employing the distributed and cooperative active response architectures [7, 8]. Currently, we can find the SSH dictionary attack related alert messages from the IDS/IPS or logging agents (sensors) in the network servers. However, with these IDS/IPS systems, we must observe directly the inbound SSH communication related packets. Further, they incur installation costs, updates of their security appliances, or network configurations.

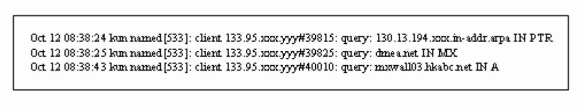
Previously, we reported that entorpy based detection in DNS traffic could be used to detect inbound- and outbound-SSH dictionary attacks [9-12]. The DNS based detection system has a merit which observes only the DNS query request packet traffic between the DNS server and its clients i.e. the DNS resolver has been already installed in almost all the network appliances like PC terminals, routers, switches, servers, network security appliances, etc. It is, however, not only difficult to calculate the thresholds but also in a high-cost for the DNS traffic or DNS traffic entropy based detection technologies [9-13].

In this paper, (1) we carried out statistical analysis on the PTR resource record (RR) based DNS query packet traffic from the campus network servers that were under inbound SSH dictionary attack through March 14th, 2009, and (2) we assessed the two suggested detection technologies by calculating the detection rate of the SSH dictionary attack, in the DNS query request packet traffic from the campus network through January 1st to December 31st, 2009.

2. Observation

2.1 Network systems and DNS query packet capturing

We investigated the DNS query request packet traffic between the top domain DNS (tDNS) server and the DNS clients. Figure 1 shows an observed network system in the present study, which consists of the tDNS server as a site local DNS cache and the SSH network servers that have a function of SSH services in the campus network, and the SSH propagation bots 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 network servers, respectively, and



```
Oct 12 08:38:24 kum named[533]: client 133.95.xxx.yyy#39815: query: 130.13.194.xxx.in-addr.arpa IN PTR
Oct 12 08:38:25 kum named[533]: client 133.95.xxx.yyy#39825: query: dmea.net IN MX
Oct 12 08:38:43 kum named[533]: client 133.95.xxx.yyy#40010: query: mxwall03.hkabc.net IN A
```

Figure 2 Structure of syslog messages generated by BIND program packages

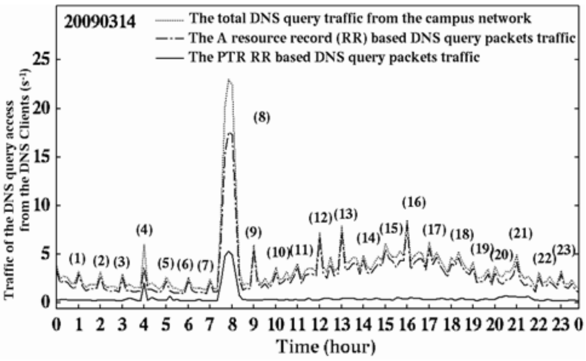


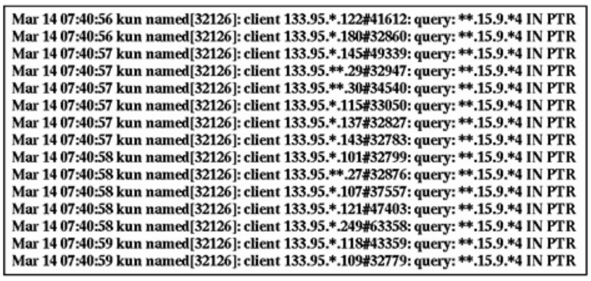
Figure 3 The total, A and PTR resource records (RRs) based DNS query request packet traffics between the top domain DNS (tDNS) server and the DNS clients on the campus network at March 14th, 2009 (s^{-1} unit)

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 program package [14]. 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 package 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 (See Figure 2).

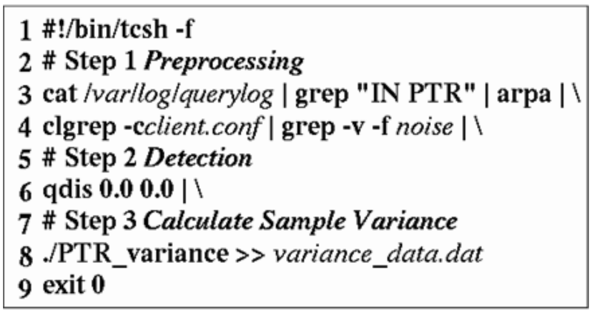
2.2 Observed DNS query request packet traffic

Firstly, we can demonstrate the observed total DNS query packet traffic, and A- and PTR-resource records (RRs) based DNS query request packet traffics from the campus network to the top domain name system (tDNS) server in March 14th, 2009, as shown in Figure 3. In Figure 3, we can find twenty three peaks



```
Mar 14 07:40:56 kun named[32126]: client 133.95.*.122#41612: query: **.15.9.*4 IN PTR
Mar 14 07:40:56 kun named[32126]: client 133.95.*.180#32860: query: **.15.9.*4 IN PTR
Mar 14 07:40:57 kun named[32126]: client 133.95.*.145#49339: query: **.15.9.*4 IN PTR
Mar 14 07:40:57 kun named[32126]: client 133.95.**.29#32947: query: **.15.9.*4 IN PTR
Mar 14 07:40:57 kun named[32126]: client 133.95.**.30#34540: query: **.15.9.*4 IN PTR
Mar 14 07:40:57 kun named[32126]: client 133.95.*.115#33050: query: **.15.9.*4 IN PTR
Mar 14 07:40:57 kun named[32126]: client 133.95.*.137#32827: query: **.15.9.*4 IN PTR
Mar 14 07:40:57 kun named[32126]: client 133.95.*.143#32783: query: **.15.9.*4 IN PTR
Mar 14 07:40:58 kun named[32126]: client 133.95.*.101#32799: query: **.15.9.*4 IN PTR
Mar 14 07:40:58 kun named[32126]: client 133.95.**.27#32876: query: **.15.9.*4 IN PTR
Mar 14 07:40:58 kun named[32126]: client 133.95.*.107#37557: query: **.15.9.*4 IN PTR
Mar 14 07:40:58 kun named[32126]: client 133.95.*.121#47403: query: **.15.9.*4 IN PTR
Mar 14 07:40:58 kun named[32126]: client 133.95.*.249#63358: query: **.15.9.*4 IN PTR
Mar 14 07:40:59 kun named[32126]: client 133.95.*.118#43359: query: **.15.9.*4 IN PTR
Mar 14 07:40:59 kun named[32126]: client 133.95.*.109#32779: query: **.15.9.*4 IN PTR
```

Figure 4 Changes in the IP address as the DNS query keywords in the total PTR resource record (RR) based DNS query request packet traffic from the campus network to top domain DNS (tDNS) server at March 14th, 2009.



```
#!/bin/tcsh -f
# Step 1 Preprocessing
cat /var/log/querylog | grep "IN PTR" | arpa | \
clgrep -cclient.conf | grep -v -f noise | \
# Step 2 Detection
qdis 0.0 0.0 | \
# Step 3 Calculate Sample Variance
./PTR_variance >> variance_data.dat
exit 0
```

Figure 5 Variance based algorithm and script code.

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 request packet traffic, while in the latter one, the total DNS query packet traffic does with the both A- and PTR-RRs based DNS query request packet traffics, simultaneously. These results indicate that we should concentrate the source IP addresses of the DNS clients at the peak (8). the total DNS query packet traffic correlates only with the A RR based DNS query request packet traffic, while in the latter one, the total DNS query packet traffic does with the both A- and PTR-RRs based DNS query request packet traffics, simultaneously. These results indicate that we should concentrate the source IP addresses of the DNS clients at the peak (8).

In the peak (8), 07:30-08:30 March 14th, 2009, the almost observed source IP addresses in the DNS query request packets are assigned to the SSH network servers in the campus network. Fortunately, we found several SSH login-failed messages in the syslog files (/var/log/secure) in the SSH network servers through 07:30-08:30 March 14th, 2009. This feature shows that the PTR RR based DNS query request packet traffic at the peak (8) can be assigned to the inbound SSH dictionary attack based DNS query request packet traffic. This is because the PTR RR based DNS query request packet traffic can be generated by the SSH server daemon program to check out their SSH clients and to log their IP addresses or fully qualified domain names (FQDNs) into the syslog files. In the peak (8), we also investigated the DNS query keywords in the PTR RR based DNS query request packet traffic and the results are shown in Figure 4. In Figure 4, we can view the scenery that the IP addresses as DNS query keyword are consecutively unchanged. Therefore, it has a possibility that this consecutive unchanged IP addresses can be useful to detect the SSH dictionary related PTR RR based DNS query request packet traffic.

2.3 Estimation of euclidian distance of IP addresses as DNS query keywords

The Euclidean distances, d(IPi, IPi-1), are calculated, as

$$d(IP_i, IP_{i-1}) = \sqrt{\sum_{j=1}^{4} (x_{i,j} - x_{i-1,j})^2} \qquad (1)$$

where both IP_i and IP_{i-1} are the current IP address i and the last IP address i-1 of the DNS query keywords, respectively, and where $x_{i,1}$, $x_{i,2}$, $x_{i,3}$, and $x_{i,4}$ correspond to an IPv4 address like A.B.C.D, respectively. For instance, if an IP address is 192.168.1.1, the vector $(x_{i,1}, x_{i,2}, x_{i,3}, x_{i,4})^T$ can be represented as $(192.0, 168.0, 1.0, 1.0)^T$. The detection is decided by thresholds d_min=0.0 and d_max=0.0, as

$$d_{min} \leq d(IP_i, IP_{i-1}) \leq d_{max} \qquad (2)$$

2.4 Estimation of sample variance for DNS query packet traffic

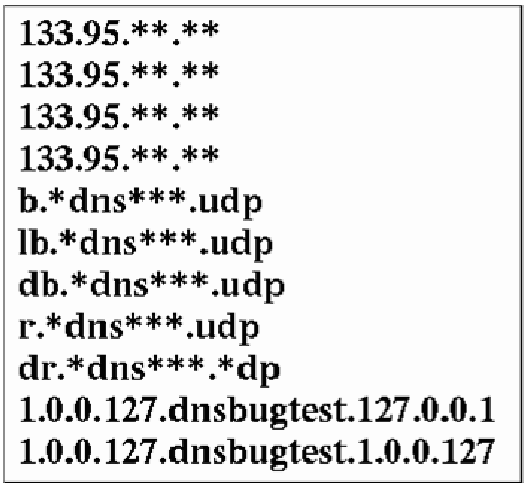
In order to observe the change in the DNS query packet traffic, we employed sample variance, as

$$s^2 = -\frac{1}{10}\sum_{i=1}^{10}(x_i - \bar{x})^2 \qquad (3)$$

where x_i is the number of the DNS query request packet traffic (min^{-1}) and $\bar{x}$ is the arithmetic mean of these DNS query request packet traffic (min^{-1}).

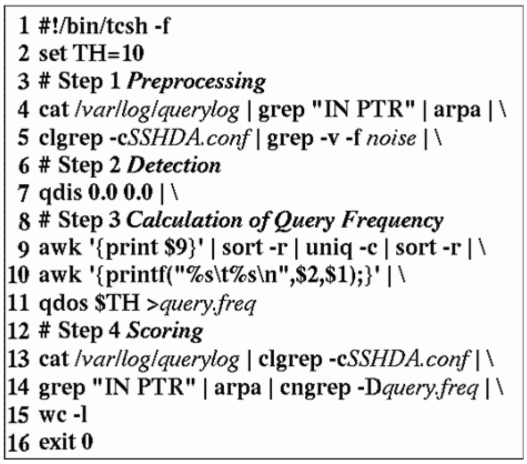
2.5 DNS traffic variance based detection algorithm for SSH dictionary attack

We suggest the following DNS traffic variance based detection algorithm of the SSH dictionary attack and we show a prototype program (see Figure 5):



```
133.95.**.**
133.95.**.**
133.95.**.**
133.95.**.**
b.*dns***.udp
lb.*dns***.udp
db.*dns***.udp
r.*dns***.udp
dr.*dns***.*dp
1.0.0.127.dnsbugtest.127.0.0.1
1.0.0.127.dnsbugtest.1.0.0.127
```

Figure 6 Noises in the PTR resource record (RR) based DNS query request packet traffic from the campus network.



```
#!/bin/tcsh -f
set TH=10
# Step 1 Preprocessing
cat /var/log/querylog | grep "IN PTR" | arpa | \
clgrep -cSSHDA.conf | grep -v -f noise | \
# Step 2 Detection
qdis 0.0 0.0 | \
# Step 3 Calculation of Query Frequency
awk '{print $9}' | sort -r | uniq -c | sort -r | \
awk '{printf("%s\t%s\n",$2,$1);}' | \
qdos $TH >query.freq
# Step 4 Scoring
cat /var/log/querylog | clgrep -cSSHDA.conf | \
grep "IN PTR" | arpa | cngrep -Dquery.freq | \
wc -l
exit 0
```

Figure 7 Signature based algorithm and script code.

Step 1: *Preprocessing*—In this step,the first grep command extracts the total PTR RR based DNS query request packet messages from the DNS query log file (*/var/log/querylog*), the arpa command converts the reverse query format ”D.C.B.A.in-addr.arpa” into the usual IPv4 format ”A.B.C.D” (A, B, C, and D represent digit numbers of 0-255), the clgrep command extracts only the DNS query traffic from the campus network, and the second grep command discards the noises shown in

Step 2: *Detection*—In the second step, the qdis command prints out a syslog message if it is calculated to be zero in the Euclidean distance,d(IPi, IP_{i-1}), between the two IP addresses IPi,IP_{i-1}, as DNS query keywords.

Step 3: *Calculate sample variance*—In the final step, the $PTR_{variance}$ command calculates the sample variance s^2(unit: 10 min^{-1})of the PTR RR based DNS query request packet traffic, employing time-sampled by ten-minute and the sampling rate is set to be one-minute (min^{-1}).

2.6 DNS traffic signature based detection algorithm for SSH dictionary attack

We suggest the following DNS traffic signature based detection algorithm of the SSH dictionary attack, in which ”signature” means the detection technology of pattern matching. We show a prototype program (see Figure 7):

Step 1: *Preprocessing*—In this step,since the first and the second grep commands, the arpa command are the same functions in the script code in Figure 5, the clgrep command extracts only the DNS query traffic from the specific SSH servers in the campus network by making reference to a signature file *SSHDA.conf*, in which the IP addresses are listed and they were observed in the PTR RR DNS query request packet traffic from the campus network through March 14th, 2009 to June 11th, 2010 (to be discussed later).

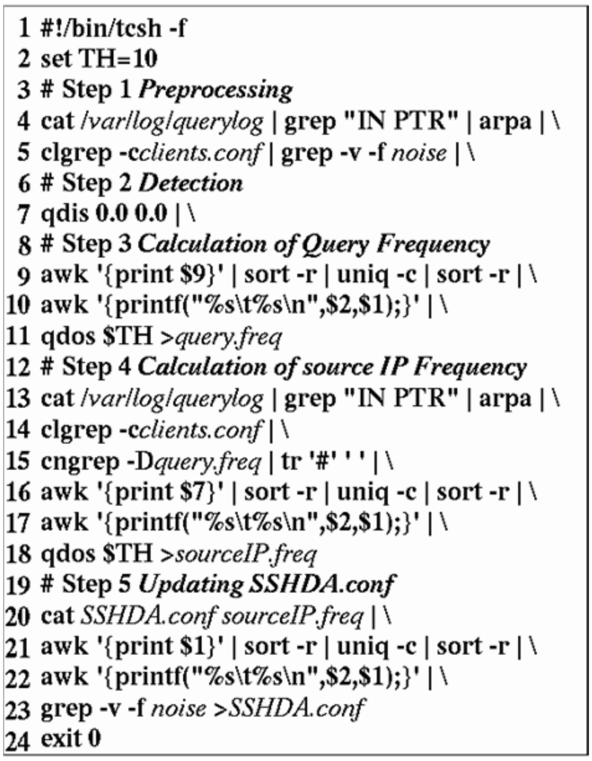
Step 2: *Detection*—In the second step, the qdis command is the same as that in Figure 5.

Step 3: *Calculation of query frequency*—In the third step, the first awk command extracts the source IP address of the SSH dictionary attacker, the two sort, uniq, and the last awk commands calculate query keyword based frequency for the PTR RR based DNS query request packet traffic, the qdos command can extract the IP address when the frequency takes more than 10 (as a threshold), and the results of this step are written in the file *query.freq*.

Step 4: *Scoring*—In the final step, the cngrep command extracts only IP address based DNS queries from the PTR RR based DNS query request packet traffic by referring to the file *query.freq*, and the wc command calculates the score for the detection.

2.7 Creating signature file

In order to obtain the IP addresses for creating the file *SSHDA.conf*, we investigated the source IP addresses in the PTR resource recode (RR) based DNS query request packet traffic including the IP addresses that were SSH dictionary attackers at March 14th, 2009 and June 15th, 2010, employing the script code (See



```
#!/bin/tcsh -f
set TH=10
# Step 1 Preprocessing
cat /var/log/querylog | grep "IN PTR" | arpa | \
clgrep -cclients.conf | grep -v -f noise | \
# Step 2 Detection
qdis 0.0 0.0 | \
# Step 3 Calculation of Query Frequency
awk '{print $9}' | sort -r | uniq -c | sort -r | \
awk '{printf("%s\t%s\n",$2,$1);}' | \
qdos $TH >query.freq
# Step 4 Calculation of source IP Frequency
cat /var/log/querylog | grep "IN PTR" | arpa | \
clgrep -cclients.conf | \
cngrep -Dquery.freq | tr '#' ' ' | \
awk '{print $7}' | sort -r | uniq -c | sort -r | \
awk '{printf("%s\t%s\n",$2,$1);}' | \
qdos $TH >sourceIP.freq
# Step 5 Updating SSHDA.conf
cat SSHDA.conf sourceIP.freq | \
awk '{print $1}' | sort -r | uniq -c | sort -r | \
awk '{printf("%s\t%s\n",$2,$1);}' | \
grep -v -f noise >SSHDA.conf
exit 0
```

Figure 8 Updater script code for SSHDA.conf file.

Figure 8).

Step 1: *Preprocessing*—In the step, all the commands are the same as those in Figure 5.

Step 2: *Detection*—In the second step, the qdis command is the same as that in Figure 5.

Step 3: *Calculation of query frequency*—In the third step, all the commands are the same as those in Figure 7.

Step 4: *Calculation of source IP frequency*—In the step, the cngrep command extracts only the PTR RR DNS query request packet traffic including the query IP addresses in the file *query.freq*, the two sort and uniq commands convert the extracted source IP addresses into the unique source IP addresses, and the last awk command writes these IP addresses and their frequencies into the file sourceIP.freq.

Step 5: *Updating of SSHDA.conf*—In the step, the first awk command extracts only IP address included in the files *SSHDA.conf* and *sourceIP.freq*, the two sort and uniq commands convert the extracted IP addresses into the unique IP addresses, and the last awk command writes these IP addresses into the file *SSHDA.conf.*

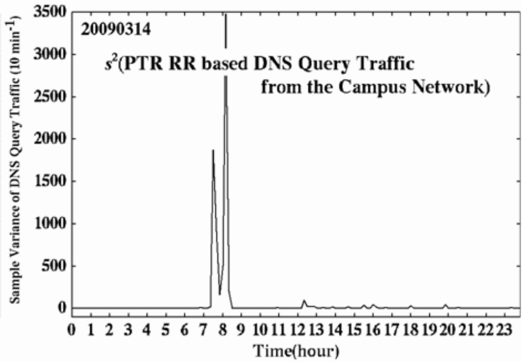


Figure 9 Changes in the sample variance of the PTR resource record (RR) based DNS query request packet traffic from the campus network to the top domain DNS (tDNS) server at March 14th, 2009 (10 min^{-1} unit).

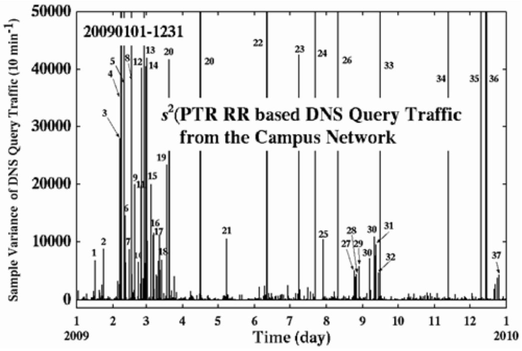


Figure 10 Changes in the sample variance of the PTR resource record (RR) based DNS query request packet traffic from the campus network to the top domain DNS (tDNS) server through January 1st to December 31st, 2009 (10 min^{-1} unit).

We carried out the script code and obtained 88 and 228 IP addresses at March 14th, 2009, and June 15th, 2010, respectively. Hereafter, we use 103 unique IP addresses as signatures for detection of the SSH dictionary attack.

3. Results and discussion

3.1 Sample variance of the PTR resource record based DNS query request packet traffic in march 14th, 2009

We illustrate the calculated sample variance of the PTR resource record (RR) based DNS query request packet traffic from the campus network at March 14th, 2009, as shown in Figure 9.

In Figure 8, we can observe two peaks through 07:30-08:30 at March 14th, 2009, and these peaks are corresponding to the peak (8) in Figure 3.

This feature suggests that it can be useful for detect-

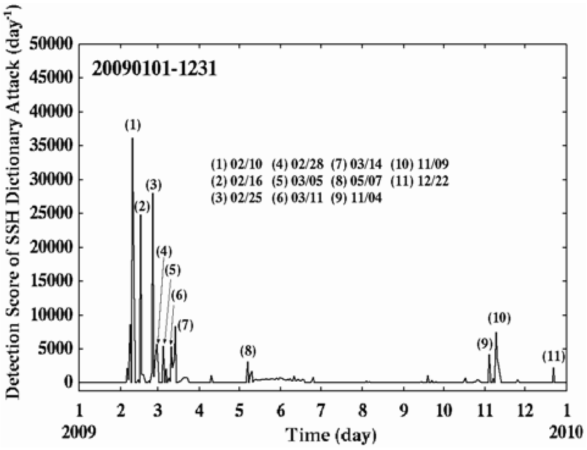


Figure 11 Changes in the signature data file based detection score of SSH dictionary attack in the PTR resource record (RR) based DNS query request packet traffic from the campus network to the top domain DNS (tDNS) server through January 1st to December 31st, 2009 (day^{-1} unit).

ing the SSH dictionary attack to the network server in the campus network by observing the changes in the variance of the DNS query request packet traffic from the networks servers.

3.2 Evaluation of variance based detection technology

Also, we show the calculated sample variance of the PTR resource record (RR) based DNS query request packet traffic from the campus network through January 1st to December 31st, 2009, in Figure 10.

Interestingly, in Figure 10, we can observe thirty-seven significant peaks in a threshold value of 5,000 (10 min^{-1}). These features represent that we can detect the inbound SSH dictionary attack to the network server in the campus network.

Previously, we reported that we assigned only nineteen peaks to the SSH dictionary attacks [12] through January 1st to December 31st, 2009. Therefore, it is concluded that at least eighteen peaks should include only false positive i.e. it has a possibility to generate a lot of false positives in the DNS traffic variance based detection technology. Furthermore, we also found false positives in the previously reported detection technology in [12].

Further studies related to DNS traffic irregularities need to be made in order to better understanding continued advancements for DNS based SSH dictionary attack detection technology.

3.3 Evaluation of signature based detection technology

We demonstrate the calculated signature based detection score (rate) for the SSH dictionary attack by observing PTR resource record (RR) based DNS query request packet traffic generated by the SSH servers in the campus network through January 1st to December 31st, 2009, as shown in Figure 11.

In this detection technology, we employed misuse intrusion detection (MID) model [15] withthe signature file *SSHDA.conf* consisting of the IP addresses which are allocated to the SSH servers in the campus network, in which the SSH servers can have a high possibility of the SSH dictionary attack from the Internet i.e. we can expect a high detection rate as well as in a lower positive manner.

As shown in Figure 11, we can find eleven significant peaks. These peaks are assigned to: (1) February 10th, (2) 16th, (3) 25th, and (4) 28th, (5) March 5th, (6) 11th, and (7) 14th, (8) May 7th, (9) November 4th and (10) 9th, and December 22nd, 2009. Interestingly, we can find several peaks through February, March, May, November, and December, 2009.

Expectedly, it is clear that the signature based detection technology gives us a precise detection rate in a low false positive manner.

However, the signature based detection needs to upgrade its signature data, frequently.

4. Conclusions

We investigated sample variance of the PTR resource record (RR) based DNS query request packet traffic from the DNS clients as the network servers which have the SSH services at March 14th, 2009, when the network servers were under inbound SSH dictionary brute force attack and we obtained the following results, as: (1) we observe the significant changes in the sample variance of the PTR RR based DNS query request packet traffic through 07:30-08:30 March 14th, 2009. It suggests that the sample variance change can be useful for detection of the inbound SSH dictionary attack, and (2) we also observed thirty-seven peaks in the sample variance change in the PTR RR based DNS query request packet traffic. However, we previously reported that the nineteen peaks were observed through January 1st to December 31st, 2009 [12]. This means that we need to develop detection technology in a lower false positive manner.

We developed signature based detection technology and evaluated by use of signature file *SSHDA.conf* in which the IP addresses corresponding to the SSH servers that there are possibilities to have an SSH dictionary attack. Fortunately, we can observe eleven significant peaks in a lower false positive manner. However, the signature based detection technology always requires updating or refreshing their pattern data. Therefore, we need near future to investigate false negative in the signature based detection technology.

Consequently, although we found that we could detect the inbound SSH dictionary attack by only observing the sample variance of the PTR RR based DNS query request traffic from the campus network, we need to continue further development of detection technology to watch the SSH dictionary attacks to the campus or enterprise network.

5. 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] D. David, C. Zou, and W. Lee, “Model Botnet Propagation Using Time Zones”, In: *Proc. of the Network and Distributed System Security (NDSS) Symposium 2006*; http://www.isc.org/isoc/conferences/ndss/06/proc-eedings/html/2006/

[5] C. Seifert, “Analyzing Malicious SSH Login Attempts”, *Technical Report, 2006* http://www.securityfocus.com/infocus/1876.

[6] D. Ramsbrock, R. Berthier, and M. Cukier, “Profiling Attacker Behavior Following SSH Compromises”, In: *Proc. of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN07)*, Washington D.C., USA, IEEE Computer Society, pp.119-124, 2007.

[7] Y. Oosumi and N. Yamai, “Technique of the countermeasure for brute force attack which can cooperate between the hosts”, *IPSJ SIG Technical Reports, Distributed System and Management 47th (DSM47)*, Vol. 2007, No. 93, pp.49-54, 2007.

[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, pp.84-89, 2008.

[9] D. A. Ludeña R., K. Sugitani, and Y. Musashi, “DNS Based Security Incidents Detection in Campus Network”, *International Journal of Intelligent Engineering and Systems*, Vol. 1, No. 1, pp.17-21, 2009.

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

[11] D. A. Ludeña R., Y. Musashi, K. Takemori, S. Kubota, K. Sugitani, T. Usagawa, and T. Sueyoshi, “DNS Based Detection of SSH Dictionary Attack in Campus Network”, In: *Proc. of the 5th International Conference on Information (INFORMATION 2009)*, Kyoto, Japan, pp.134-137, 2009.

[12] D. A. Ludeña R., Y. Musashi, K. Takemori, S. Kubota, K. Sugitani, T. Usagawa, and T. Sueyoshi, “DNS Based Detection of SSH Dictionary Attack in Campus Network,” *Information*, Vol. 13, No. 3(A), pp.701-707, 2010.

[13] K. Takemori, D. A. Ludeña R., S. Kubota, K. Sugitani and Y. Musashi, “Detection of NS Resource Record DNS Resolution Traffic, Host Search, and SSH Dictionary Attack Activities”, *International Journal of Intelligent Engineering and Systems*, Vol. 2, No. 4, pp.35-42,2009.

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

[15] D. E. Denning, “An Intrusion-detection model”, *IEEE Trans. Soft. Eng.*, Vol. SE-13, No. 2, 1987, pp. 222-232.