Detection of Bot Worm-Infected PC Terminals

Dennis A. Ludeña Romaña,
Graduate School of Science and Technology
Kumamoto University, 860-8555, JAPAN
dennis@st.cs.kumamoto-u.ac.jp

Yasuo Musashi, Ryuichi Matsuba and Kenichi Sugitani
Center for Multimedia and Information Technologies
Kumamoto University, 860-8555, JAPAN
{musashi,matsuba,sugitani}@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 record 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. 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, Bot Network, Spam Mail, Service Attack Worm

1 Introduction

Recent internet worms, especially a bot worm (BW) becomes one of the big threats in the information- and communication-technology (ICT) based society[1]. This is because the BW has a lot of functions like a spam mailing, a distributed denial-of-service (DDoS) attack, and information theft. Also, it infects with the next victim PC terminals by acting as mass mailing worm (MMW) and/or service attack worm (SAW)[2].

Previously, we reported that the client MX record based DNS query packet access showed the DNS resolution access from the MMW-infected PC terminals and the abnormal random TCP session trial access to the ports of 135, 139, and/or 445 from the SAW-infected PC terminals[3].

The present paper discusses on the investigation of (1) the abnormal A record based DNS query access from the W32/Mytob.A BW-infected PC terminal at 25th February, 2005, (2) the illegal TCP session trial access from the SAW-infected PC terminals, and the client MX record based DNS query access through 1st January, 2005 to 31st March, 2006.

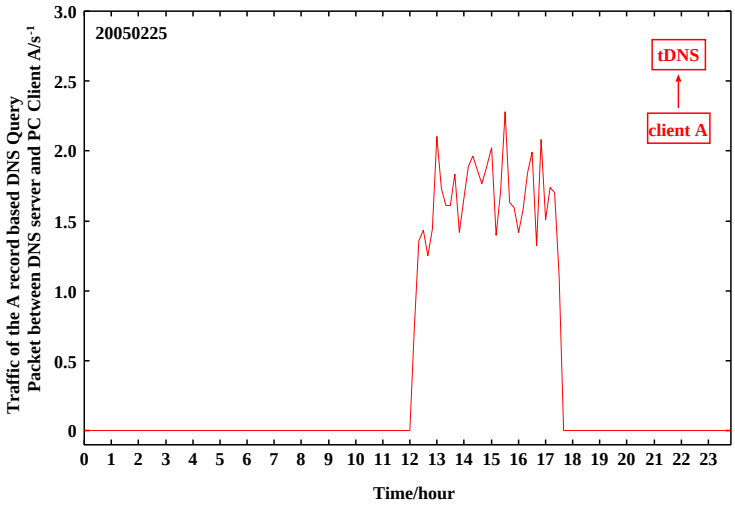

Figure 1. Traffic of the A record based DNS query packet access between the top domain DNS (**tDNS**) server and the DNS client A at 25th February, 2005 (s^{-1} unit).

2 Observations

We investigated traffic of DNS query access between the top domain DNS server (**tDNS**) [1] and DNS clients. In **tDNS**, BIND-9.2.6 program package has been employed as DNS server daemon[4]. The DNS query packets and their query contents have been captured by a query logging option (see man named.conf). The log of DNS query access has been recorded in the syslog file. All of the syslog files are daily updated by the crond system. The TCP session trial packets were recorded by the iplog-2.2.3 packet logger program package[5]. We observed traffic of DNS query request packet from DNS clients to the top domain name server (**tDNS**).

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 2. Statistics of the contents for the A record based DNS query packets from the client A at 25th February, 2005.

3 Results and Discussion

Firstly, we observed traffic of the A record based DNS query packets from a DNS client A to the top domain DNS (**tDNS**) server through the day of 25th February, 2005 (Figure 1), because the client A is one of the top DNS query access clients in the day. In Figure 1, the traffic starts from 12:00 and ends after

[1] **tDNS** is a secondary top domain DNS server in Kumamoto University (kumamoto-u). The OS is Linux OS (kernel-2.4.32), and hardware is an Intel Xeon 2.40GHz Dual SMP machine.

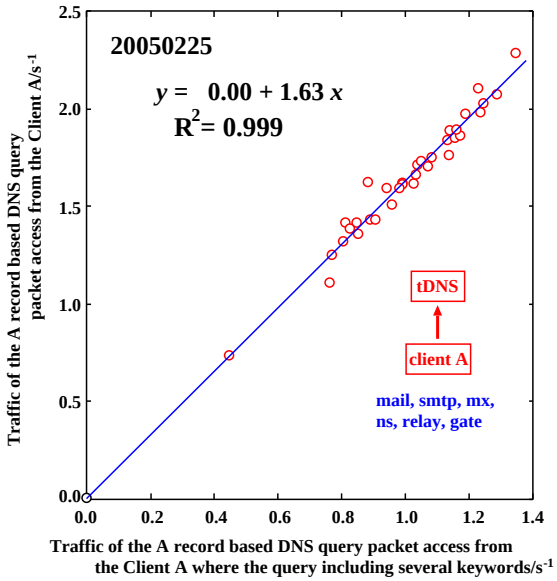

Figure 3. Total traffic of the A record based DNS query packet access from the client A versus traffic of the A record based DNS query packet access from client A where including the six keywords at 25th February, 2005 (s^{-1} unit).

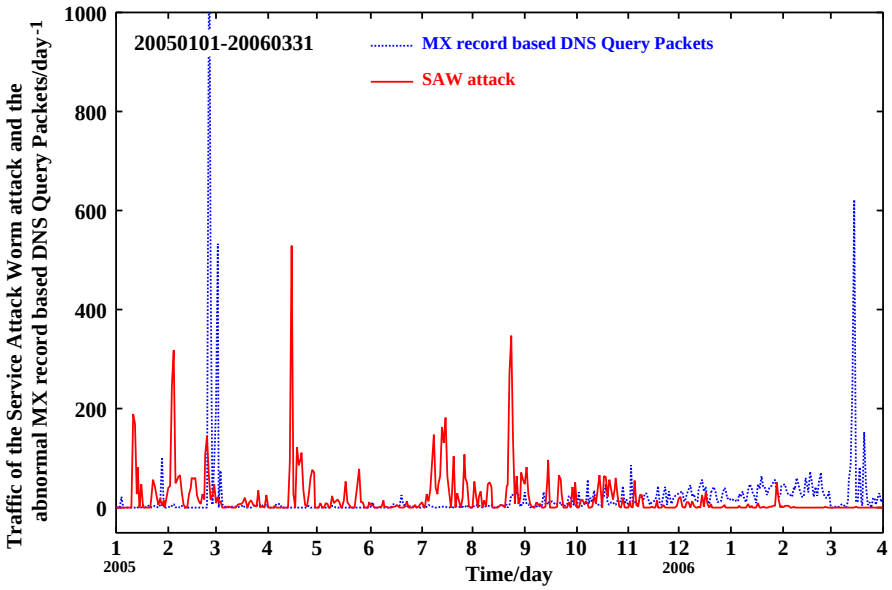

Figure 4. Traffic of the abnormal MX record DNS query packets and traffic of TCP session trial access from the service attack worm (SAW)-infected PC terminals (day^{-1} unit).

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 record based DNS query packets, and the PTR record based ones, are obtained to be 32,728/day, 32,721/day, and 7/day, respectively, and no MX record based packet can be observed. This result shows that the total DNS query access traffic from the client A almost consists of the A record based DNS query access traffic. We

can demonstrate statistics of the query contents for the A record based DNS query packets from the client A at 25th February, 2005 (Figure 2). In Figure 2, the keywords of "mail", "smtp", "mx", "ns", "gate", and "relay" are used to generate fully qualified domain names of the E-mail servers that have ever been observed when detecting IP addresses of the W32/Mydoom MMW-infected PC terminals[3], *i.e.* the PC client A is probably infected with a new type of mass mailing worm (MMW) which resembles well W32/Mydoom variants but they send no MX record based DNS query packet. This new worm was assigned to be the W32/Mytob.A bot worm (BW) after 27th February, 2005 by several anti-virus vendors[2]. Figure 3 shows regression analysis on the total traffic of the A record based DNS query packet access from the client A versus that of the A record DNS query packet access from the client A including the six keywords. The data 25th February, 2005 and the correlation coefficient (R^2) is 0.999.

In Figure 4, we illustrate both traffic curves of the MX record based DNS query packets and the TCP trial session access like the ports of 135, 139, and 445 from the service attack worm (SAW)-infected PC terminals through 1st January, 2005 to 31st March, 2006. Interestingly, the both traffic curves start synchronizing after 23rd August, 2005 to 27th February, 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[2].

4 Concluding Remarks

We investigate statistically the DNS traffic between the top domain DNS server (**tDNS**) and its DNS clients. It can be concluded that the A record based DNS query packet access from the W32/Mytob BWs-infected PC terminals includes the six keywords and the traffics of abnormal MX record based 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 client A and MX records based DNS query packets and TCP session trial like port 135, 139, and 445, like SAWs.

References

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

[2] (a) http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYTOB.A (b) http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_ZOTOB.{A-X}

[3] Y. Musashi, R. Matsuba, and K. Sugitani, Indirect Detection of Mass Mailing Worm-Infected PC terminals for Learners, *Proceeding for the 3rd International Conference on Emerging Telecommunications Technologies and Applicatications (ICETA2004)*, Kosice, Slovakia (2004) 233–237.

[4] http://www.isc.org/products/BIND/

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