Building an Anti-Botnet Platform to Mitigate Botnet

SHIAN-SHYONG TSENG[1,2], AI-CHIN LU[2],
NAI-WEN HSU[2], GENG-DA TSAI[2], CHING-HENG KU[2]
[1]Dept. of Applied Informatics and Multimedia, Asia University
[2] Taiwan Network Information Center
TAIWAN
{sstseng, aclu, snw, dar, chku}@twnic.net.tw

Abstract- In recent years, with the rapid growth of the Internet applications and services, botnet becomes one of the most severe threats on the Internet. Because the botnets can be automatically evolved as different localized versions in a short period of time, how to find an effective and efficient approach to detect and notify the Botnet attack becomes an important and interesting issue. To cope with the issue, we proposed a collective intelligence approach which aims to enable the systematic and dynamic creation of malware information and knowledge. Accordingly, we developed an anti-botnet platform together with a social networking structure, and an anti-botnet service web site, where the collaborative anti-botnet platform is used to collect the Botnet attack information through the Honeypot Deployment of different organizations and the proposed social networking structure can help build the consensus to select the attributes of the Botnet. The collected data can be then sent to the Anti-Virus Software Vendor to develop the antidote which can be free downloaded by the infected Internet users. Besides, an anti-botnet web site is also developed for Botnet information query, and malware prevention teaching. According to the experimental results, we show that the platform can be used to reduce the Botnet and malware attacks, and the collected information and knowledge can be used to enhance the national information and communication security.

Key-Words: - Anti-Botnet Platform, Honeypot, Botnet, collective intelligence, social networking, consensus building

1 Introduction

1.1 Background and Motivation

The development of network technology brings the convenience of the communication between people, but the issues of the information security caused by a variety of system vulnerability or weaknesses are increasing dramatically.

In all kinds of new Internet-based intrusion attack, one of the greatest damages is so-called the Botnet attacks, commonly known as "zombie network" or the "robot network". Bot attacks which often happened with the e-mail, instant messaging or the computer system vulnerabilities to hack computers are hidden in the program of the computer[1], and the infected computers with the bot invasion are connected as the botnet. The behavior of Botnet viruses is different from the original Trojans, where the original Trojans only attack a specific target, but the Botnet just like worm can slowly spread in the network space and trigger the computer attack by itself when it finds the vulnerabilities of the computer [2].

Because the botnets can be automatically evolved as different variants in a short period of time, how to find an effective and efficient approach to detect and notify the Botnet attack is our concern. In this paper, we proposed an anti-botnet platform [3] which can collaboratively collect the Botnet attack information through the Virtual Honeypot deployment of different organizations including TWCERT/CC, governmental and commercial ISPs [4]. The collected data can be then sent to the Anti-Virus Software Vendor [5] to develop the antidote which can be free downloaded by the infected Internet users, where the related ISPs help to notify the Botnet attack for the users.

1.2 Related work

According to the Symantec Global Internet Security Threat Report[6], overall in 2011, botnets produced approximately 81.2% of all spam in circulation. With the power of botnets, robot networks of computers infected with malware and under the control of cybercriminals, spammers can pump out billions of spam emails every day, clogging-up company networks and slowing down communications. There were, on average, 42 billion spam messages a day in global circulation in 2011, compared with 61.6 billion in 2010. Hence, Botnet takedowns can reduce Spam volumes. For example,

the overall number of spam fell consider-ably in the year from 88.5% of all email in 2010 to 75.1% in 2011. This was largely thanks to law enforcement action which shut down Rustock, a massive, worldwide botnet that was responsible for sending out large amounts of spam. On March 2012, Microsoft and US law enforcements took down the Rustock botnet. Besides, FBI awarded court order to shut down the Coreflood botnet by sending a "delete" command (included in the threats design) to compromised computers on April 2012.

As to the Botnet attack detection and prevention, the Japanese Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy,Trade and Industry (METI) launched the Cyber Clean Center plan that is implemented by the Telecom-the ISAC Japan, and JPCERT / CC and IPA, where 76 ISPs and anti-virus software industry are involved[7]. Besides, Hailong Wang[8] proposed the Role-based collaborative information collection model for Botnet detection.

In order to mitigate the Botnet efficiently and effectively, our basic idea is to standardize both the communication protocol of the collected Botnet attack information and the process of the data transmission through social networking. Accordingly, our proposed anti-Botnet platform consists of the following steps: the detection and collection of the Bot, the classification of the bot, the development of the antidote of the bot, the notification of the infected users, and the provision of the downloadable antidote.

To evaluate the effectiveness and the efficiency of the anti-Botnet platform, the proposed procedure in the anti-Botnet platform has been successfully examined in Taiwan. The results show that the domestic infection proportion, which is the ratio of the infective domestic IP addresses and infective global IP addresses, is gradually reduced. It means that the platform can effectively reduce the number of Bots.

2 Social Networking Structure

2.1 Bot Collection based on the Cooperation among the Social Networking Groups

A social networking is a social structure made up of a set of actions (such as individuals or organizations). In the proposed social networking structure, as shown in Figure 1, five groups including TANet CERT, TWNCERT, NCC-CERT, TWIA, and TWCERT/CC form Taiwan Security Alliance, where TWCERT/CC plays the role of coordinator and each group may consist of several members deploying Honeypots. Through the cooperation among all the members, the mission of the Bot collection in our anti-Botnet platform can be easily achieved.

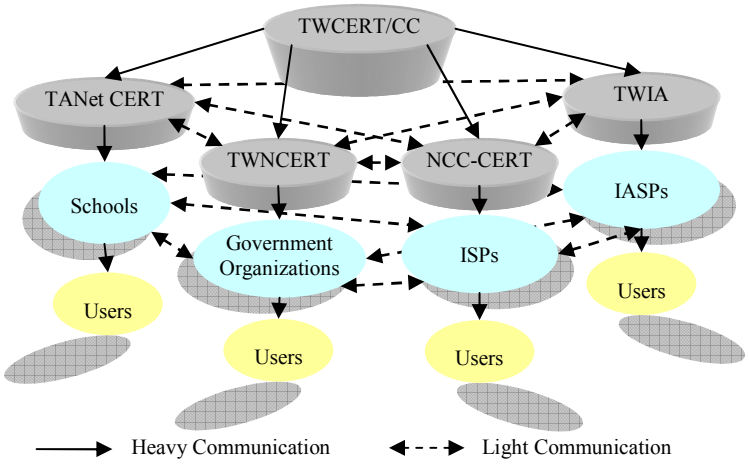

Figure 1. The Groups of Social Networking Structure

2.2 Consensus Building of the attributes of the Botnet

To collect Botnet attack information efficiently, our idea is to standardize the communication protocol of the collected Botnet attack information collaboratively. During the consensus building process of the selection of the attributes of the data schema for the malware information, the privacy issue is most concerned for different groups in our social networking structure.

Besides, the attributes of the instance of the attack event are also selected by the groups. These attributes will be used to build the antidote database for user downloading.

In this study, the consensus is reached through the heavy communication and the monthly discussion by the proposed social networking structure. We finally select nine useful attributes of the Botnet from the 31 attributes in the Honeypot database as shown in the following.

Field	Data Type	Description
malware_id	integer(4)	malware sample serial number
hash_sha512	Character (128)	Hash sha512
hash_md5	Character(32)	Hash MD5
first_collection_time	timestamp with time zone	acquired time of the malware sample

ISBN: 978-1-61804-109-8

malware_content	String	content of the malware sample
malware_download_site	string(512)	download site of the malware
attack events sequence	<(inet$_1$,inet$_1$,timestamp$_1$), (inet$_2$,inet$_2$,…), (…)>	each attack event in the sequence includes honeypot IP, source IP address of the attack event, and time of the attack event

3 Architecture of Anti-Botnet Platform

As we know, the Virtual Honeypot is a security resource whose value lies in being probed, attacked or compromised. In this section, we are concerned with how to collect more Bot data from a variety of program data sources and how to efficiently provide the antidote.

As we know, Nepenthes, a low-interaction Honeypot, can simulate the known vulnerabilities. Therefore, when the malicious code attacks these weaknesses, the information of the malware can be automatically stored. In the process of the collection of Bot, the collaboration of the members of our social networking structure that deploy honeypots in different locations can help simultaneously collect the malware and the attack information from different organizations.

Based upon the consensus of the attributes of the Bots, we developed an anti-botnet platform to collect the Botnet attack information through the Nepenthes Honeypot Deployment of different organizations.

The Anti-Botnet platform consists of four major steps as shown in Figure 2.

Step 1: Filter the Bot instances having antidote using the Bot signature (MD5) matching method.

Step 2: Develop the antidote for the new Bot found in Step 1.

Step 3: ISPs make the user notification for the infected users.

Step 4: Provide the antidote and maintain the antidote DB.

3.1 Filtering the Bot instances having Antidote

To classify the collected malware instances into the ones having antidote and the ones not having antidote, the signature, such as the MD5 data, of the new Bot instance is compared with those of the bots having antidotes. If matched, we send the IP addresses, timestamp, antidote download URL to ISPs. The ISP will then notify the user to download the antidote. Otherwise, the sample, timestamp, and MD5 code will be sent to the anti-virus vendor for developing the antidote.

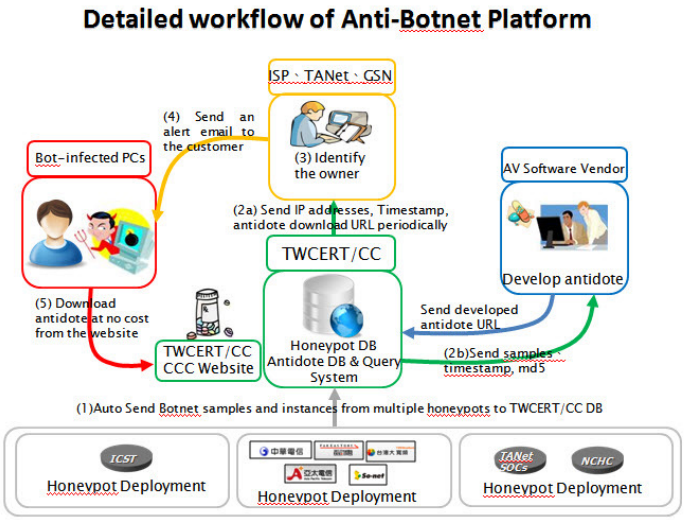

Figure 2. The workflow of the process in the Anti-Botnet Platform

3.2 Deployment of the Antidote

In the process of developing the antidote, the Anti-virus company joining our project used the sand box method to develop the antidote for the new Bot. The produced antidote is sent back to the TWCERT / CC and stored into antidote DB site for the users to download.

In the last two years, the statistics results show that the average antidote developing time is about 2 days and the detoxification rate is more than 95%.

3.3 User Notification

After receiving the notification of the information of the antidote, the ISP will notify the corresponding user to download the antidote.

In the process of the user notification, we design the automatic notification system to immediately notify ISPs, and the ISP can then efficiently notify the user within 8 hours.

4 Anti-Botnet Service Web site

With the supports of the social networking groups, an anti-botnet web site is further developed for Botnet information query, the antidote download,

ISBN: 978-1-61804-109-8

and malware prevention teaching.[3] After the users downloaded the antidote and removed the Bot from the infected computer, we also provide the related knowledge of the antidote to them. Besides, the real-time information update and the on-line help are also provided in this web site.

In order to increase the users' Botnet knowledge, four kinds of learning contents are provided on the web site, such as

(1) Software Security, including the installation of anti-virus software and software upgrade,
(2) Device Security, including how to enable firewall and setup the configuration, protect against any malicious programs trying to attack via USB drive,
(3) Network Security, including using private IP address to increase the level of the security, and
(4) User Behavior Security, including must-not-visit and the untrusted URL, to avoid opening the unknown email, and change password frequently.

5 Performance Analysis of Anti-BOTNET platform

We had implemented the anti-BOTNET platform prototype to collect Bot information and produce the corresponding antidote since July 2011. At the end of 2011, this platform started to notify the relevant users to download the antidote for the removal of the malware.

In order to evaluate the performance of the anti-Botnet platform, the following analyses have been done.

5.1 Analysing the service ports of collected instances

To know how many of the infected sites are servers, we have scanned over 35,000,000 domestic IPv4 addresses to see whether a service port, such as DNS, Web and mail service of the site is on. Compared the results with the IPs of Bot instances, we can determine the infective site is a server or a client. We therefore found that 98% of the infected sites without opening the service ports are regular personal computers. This is consistent with our intuition; the security protection level of user's computer is usually lower than that of the server.

5.2 Analysis of the Infection rate of Botnet

In order to know the effectiveness of the anti-Botnet platform, we calculate the proportion of infective domestic IP addresses R_t in infective global IP addresses as follows.

$$R_t = \frac{N_t}{N_f + N_t}, \text{ where}$$

N_t : *number of Infective IP addresses in Taiwan*

N_f : *number of Infective foreign IP addresses*

Until April 2012, there are more than 15,900,000 instances are collected from 59,591 foreign sources (IP addresses) and 16,285 of them are domestic IP addresses, about 27%, as shown in Figure 3. It can be seen that the proportion of the infective domestic IP addresses is gradually reduced. It shows that our platform can effectively reduce the number of Bots.

5.3 Statistics of the antidote developing time

We analyze the time elapsed in the development of the antidote to show the efficiency of the antidote development. Besides, the download rate of the antidote is also proposed.

As to the collected 19,235 malware samples including 629 unsolved sample, the antidote production rate is 96.7%. Besides, 66.3% of the antidotes can be developed within one day.

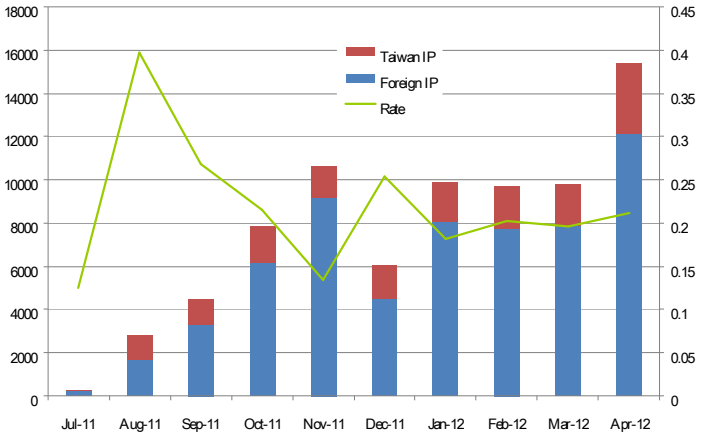

Figure 3: Source IP of instances and the proportion of the infective domestic IP addresses and infective global IP addresses.

5.4 Analysis of BOTNET malware categories

To find the development trends and the Bot behavior within the infective range for the mitigation of Bot[9][10], twelve categories of the malware including 18606 malware samples are classified as shown in Figure 4[11]. According to the statistics, we found that 86% of malwares have

been downloaded by the http protocol and 86% of them are with the execution file.

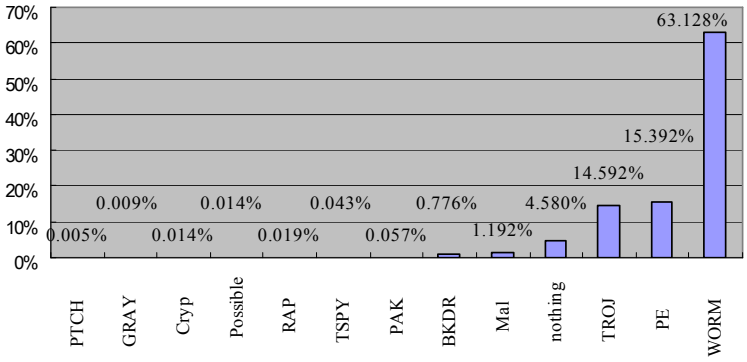

Figure 4: The proportion of the type of the collected malware

6 Conclusion

In this paper, we successfully proposed a collective intelligence approach which aims to enable a systematic and dynamic creation of malware information and knowledge.

Accordingly, we developed an anti-botnet platform together with a social networking structure, and an anti-botnet service web site, where the collaborative anti-botnet platform is used to collect the Botnet attack information through the Honeypot Deployment of different organizations.

The proposed social networking structure can successfully help build the consensus to select the attributes of the data schema of the Botnet and collaboratively collect the Bots. Besides, an anti-botnet web site is also developed for Botnet information query, and malware prevention teaching.

According to the experimental results, we show that the platform can be used to reduce the Botnet and malware attacks.

To evaluate the effectiveness and the efficiency of the anti-Botnet platform, the proposed procedure in the anti-Botnet platform has been successfully examined in Taiwan. The results show that the domestic infection proportion, which is the ratio of the infective domestic IP addresses and infective global IP addresses, is gradually reduced. It means that the platform can effectively reduce the number of Bots.

In the near future, we will continuously improve this anti-botnet platform service to mitigate the variant Bots in Taiwan.

.

Acknowledge

This paper is partially sponsored by the Taiwan Network Information Center (TWNIC) and TWCERT/CC.

References:

[1] Workshop on Understanding Botnets of Taiwan 2011 (BoT 2011), http://ntu.botnet.tw/BoT2011/

[2] Hacks In Taiwan Conference, http://hitcon.org/hit2011/

[3] Cyber Clean Center Taiwan, https://ccc.cert.org.tw/

[4] Taiwan Internet Association, http://www.twia.org.tw/

[5] Trend Micro, http://www.trendmicro.com/

[6] Symantec, “2011 Trends of Internet Security Threat Report”, Volme 17, April 2012.

[7] Cyber Clean Center Japan, https://www.ccc.go.jp/

[8] Hailong Wang; Zhenghu Gong, Role-based Collaborative Information Collection Model for Botnet Detection, Collaborative Technologies and Systems (CTS), 2010 International Symposium Page: 473-480

[9] Ming-Zong Huang; Chia-Mei Chen, Hybrid Botnet Detection, http://ndltd.ncl.edu.tw/cgi-bin/gs32/gsweb.cgi?o=dnclcdr&s=id=%22098NSYS5396050%22.&searchmode=basic

[10] Tung-Ming Koo, Hung-Chang Chang, Quan-Wei Guo, 2011, Construction P2P firewall HTTP-Botnet defense mechanism, 2011 IEEE International Conference on Computer Science and Automation Engineering, 2011/06/10-12, IEEE, Shanghai, China.

[11] Virus Total, “Free Online Virus, Malware and URL Scanner”, http://www.virustotal.com/