

Botnet Detection by Abnormal IRC Traffic Analysis

Gu-Hsin Lai¹, Chia-Mei Chen¹, and Ray-Yu Tzeng², Chi-Sung Laih²,
Christos Faloutsos³

¹National Sun Yat-Sen University Kaohsiung 804, Taiwan

²National Cheng Kung University, Tainan, Taiwan

³Carnegie Mellon University, Pittsburgh, USA

agl@cm.nsysu.edu.tw

Abstract. Recently, Botnet has become one of the most severe threats on the Internet because it is hard to be prevented and cause huge losses. Prior intrusion detection system researches focused on traditional threats like virus, worm or Torjan. However, traditional intrusion detection system cannot detect Botnet activities before botmasters launch final attack. In Botnet attack, in order to control a large amount of compromised hosts (bots), Botmasters use public internet service as communication and control channel (C&C Channel). IRC (Internet Relay Chat) is the most popular communication service which botmasters use to send command to their bots. Once bots receive commands from botmasters, they will do the corresponding abnormal action. It seems that Botnet activities could be detected by observing abnormal IRC traffic.

In this paper, we will focus on abnormal IRC traffic analysis, we will use three unique characteristics of Botnet, "Group Activity", "Homogeneous Response" and "Abnormal direction of PING and PONG messages" to detect abnormal Botnet activities in LAN. We develop an on-line IRC IDS to detect abnormal IRC behavior. In the proposed system, abnormal IRC traffic can be detected and we can (1) identify the infected hosts (bots) before botmasters launch final attack (e.g. DDoS or Phishing) and (2) find out the malicious IRC servers in LAN in real time. The experiments shows that the proposed system can indeed detect abnormal IRC traffic and prevent Botnet attack.

Keywords: Botnet, Intrusion Detection System, IRC

¹ Acknowledgement: This work was supported in part by TWISC@NCKU and iCAST, National Science Council under the Grants NSC 97-2219-E-006-009 and NSC97-2745-P-001-001

1 Introduction

Bot virus is a kind of malware, an infected host will follow the instructions which are sent by remote botmasters. There are three stages in Botnet attack, they are infection stage, communication stage and attack stage. Figure 1 illustrates the attack process of Botnet.

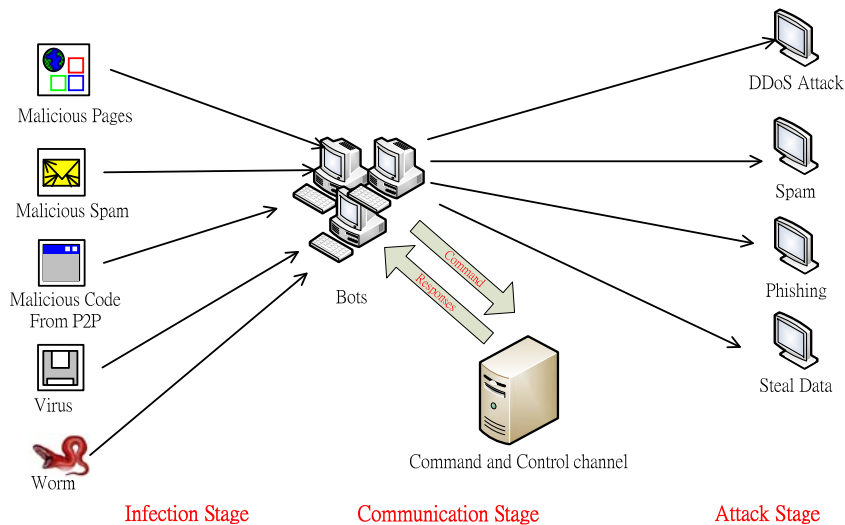


Figure 1: Process of Botnet attack

In the beginning, bot viruses are spread via malicious pages, malicious spam, malicious software in P2P, virus or worm. Once a host is infected, it becomes a bot. Then botmasters uses some public service as command and control channel to communicate with their bots and launch attack. In figure 1, we can see the complexity of Botnet attack. Attackers can use various ways to compromise hosts and attack victims. Prior works focused on detecting abnormal behavior in infection and attack stage. However, it is too difficult for an intrusion detection system to detect so many types of attack. In addition, even an intrusion detection system can detect abnormal behavior in attack stage, victims might already suffer from losses.

Botnet attack is hard to prevent because (1) it has incubation period and (2) the attack scenario is unexpected. In traditional worm attack, compromised hosts will generate abnormal traffic once they are infected. Different from traditional worm or

virus attack, bots do not have any abnormal behavior. Therefore, intrusion detection systems are unable to detect abnormal behavior of bots in early stage. Moreover, some bot viruses are spread via spam mails or malicious web pages to evade intrusion detection systems. It seems that it is hard to detect “all” abnormal behaviors in infection and attack stage. Compared with infection and attack stage, abnormal behaviors of bots in communication stage is relatively stable and unlikely to change among bots and their variants. Therefore, developing an intrusion detection system for observing, analyzing and detecting abnormal C&C channel traffic is needed.

Botmasters can use either passive or active C&C channels to transmit command to their bots. In passive C&C channel, botmasters put their commands into a file and bots would access this file periodically. A typical example of passive C&C channel is http-based C&C channel, botmasters put their command in web servers as a web page or a file. Bots would download the command file or browse the web page periodically and follow the instructions. In active C&C channel, botmasters send commands to actively in real time. A typical example of active C&C channel is IRC-based C&C channel, bots would connect to a specific IRC server to receive command from botmasters. Most botnet use active C&C channels because they can fully control their bots in real time.

IRC service is the most popular C&C channel which Botnet use. IRC is a form of real-time Internet text messaging (chat) or synchronous conferencing. It is mainly designed for group communication in discussion forums, called channels, but also allows one-to-one communication via private message. Bots will connect to a pre-defined IRC channel waiting for botmaster’s command. Figure 2 illustrates an example of IRC channel which Botnet uses.

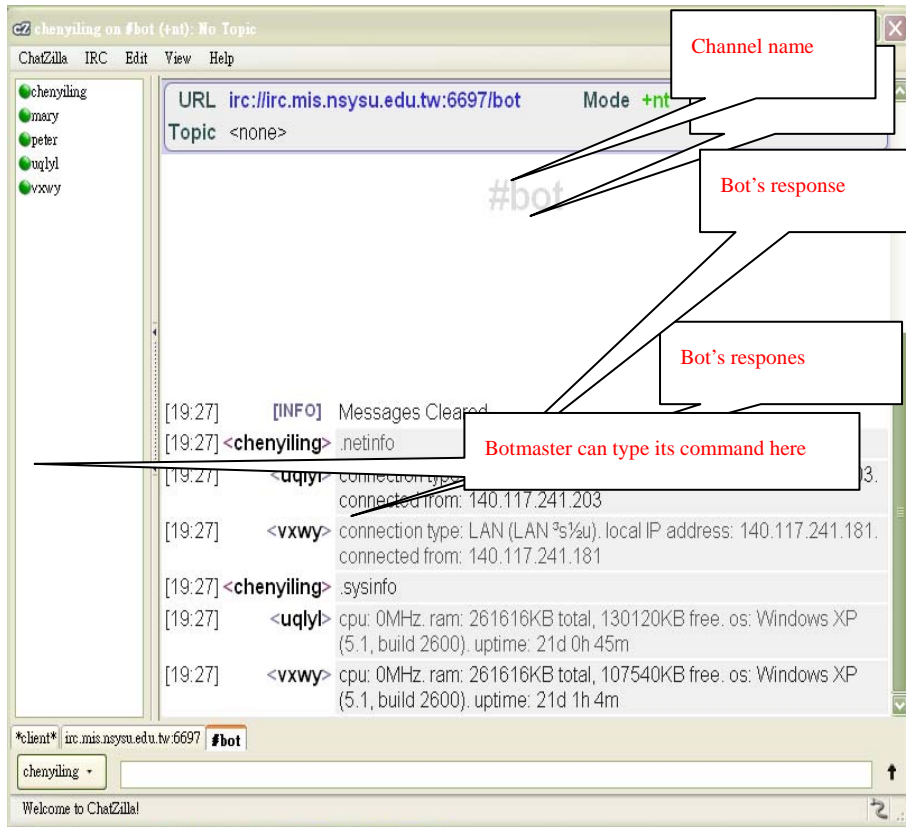
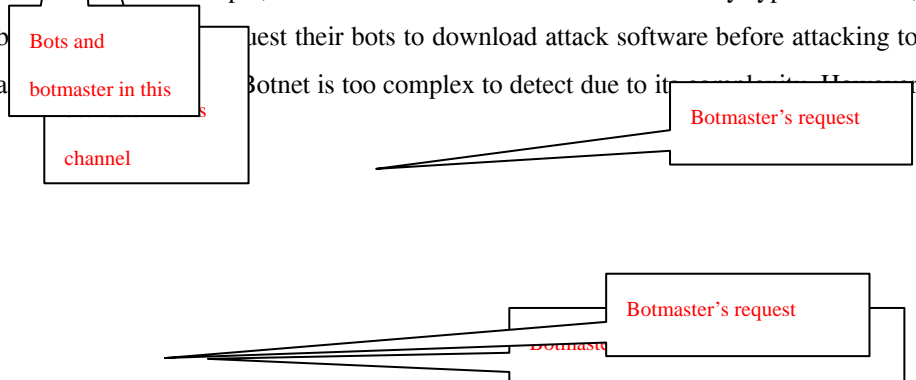


Figure 2: An example of Botnet Channel

Figure 2 illustrates how Botnet works in an IRC channel. In this example, there are two bots (uqlyl and vxwy) and a botmaster (chenyiling) in a channel called “bot”. Bots always connect to this channel waiting for the command from botmaster. Once bots receive the command from botmaster, they will follow the command and respond immediately. In this example, botmaster request its bots to provide their network and system information and bots response immediately.

In above example, we can see that botmaster can launch any types of attack, botmaster can request their bots to download attack software before attacking to a target. Botnet is too complex to detect due to its distributed nature.



if we can detect abnormal IRC traffic, we can identify the suspicious hosts and prevent Botnet rather than detect Botnet. In this paper, we observe the unique characteristics of Botnet's IRC traffic and develop an on-line IRC intrusion detection system to detect abnormal IRC traffic. Based on our observation, there are three unique characteristics in Botnet's IRC traffic, they are (1) group activity, (2) homogeneous response and (3) abnormal the direction of PING and PONG. Using these unique characteristics, the proposed system can detect abnormal IRC traffic in communication stage.

The next section describes related work on IRC Botnet intrusion detection systems. Section 3 describes how group activity, homogeneous response and abnormal direction of PING and PONG messages are used to detect abnormal IRC traffic. The proposed system is demonstrated in section 4. Experiment result is presented in section 5. Section 6 discusses advantages of our approach and future work.

2 Literature Review

In this section, we survey some prior intrusion detection of IRC-Botnet.

Gu et al. proposed a system called "Botsniffer" which detect abnormal group activities and response [2]. Botsniffer used sequential probability ration testing to calculate a comprehensive anomaly score when observing a sequence of group activities and response [7]. However, this work assumed that every rroup activities and response is i.i.d. and Botsniffer needed some prior knowledge about the conditional probability. Thus Botsniffer seems not practical. Choi et al. proposed a Botnet detection mechanism to detect abnormal group DNS query [1]. They thought that bots always use domain name rather than IP address to connect to C&C server to enhance the migration of C&C servers. Before bots connect to their C&C server, bots need to get the ip address of C&C servers by DNS query. Villamarin-Salmon et al. proposed a Bayesian approach to detect bots based on the similarity of their DNS traffic.[6] Detection of abnormal DNS query in a LAN is not practical. Because in a LAN, it's common for a group of normal hosts which have similar DNS traffic (e.g. Query ip

address of a public server like Google). Moreover, it is also hard to get complete DNS logs. Therefore, Using DNS query behavior to detect Botnet activities in a LAN is not practical. Ji et al. proposed a Botnet detection and response framework which use data provided by ISPs.[3] The proposed approach needed a lot of integrated data from ISPs and it is almost impossible to practice. Takemori et al. proposed a cooperative framework which could trace wictim-to-bot and bot-to-C&C traffic.[4] However, their approach was too complex to build. It is an ISP-level framework not a organization level solution.

It seems that there are only few researched which tried to detect Botnet activities in a local area network. Therefore, a novel on-line abnormal C&C traffic detection mechanism is needed.

3 Proposed Approach

In this paper, we design an IRC intrusion detection system to observe abnormal IRC traffic in LAN. The goals of the proposed systems are (1) to detect the infected hosts in a LAN; (2) to detect the suspicious IRC servers in LAN; (3) to detect the IP address of botmasters if botmasters use internal IRC servers; (4) to detect the IP address of external C&C servers. Figure 3 and 4 illustrate the environment of the proposed system. Figure 3 illustrates the situation which IRC Server is outside of LAN and Figure 4 illustrates the situation which IRC Server is within LAN.

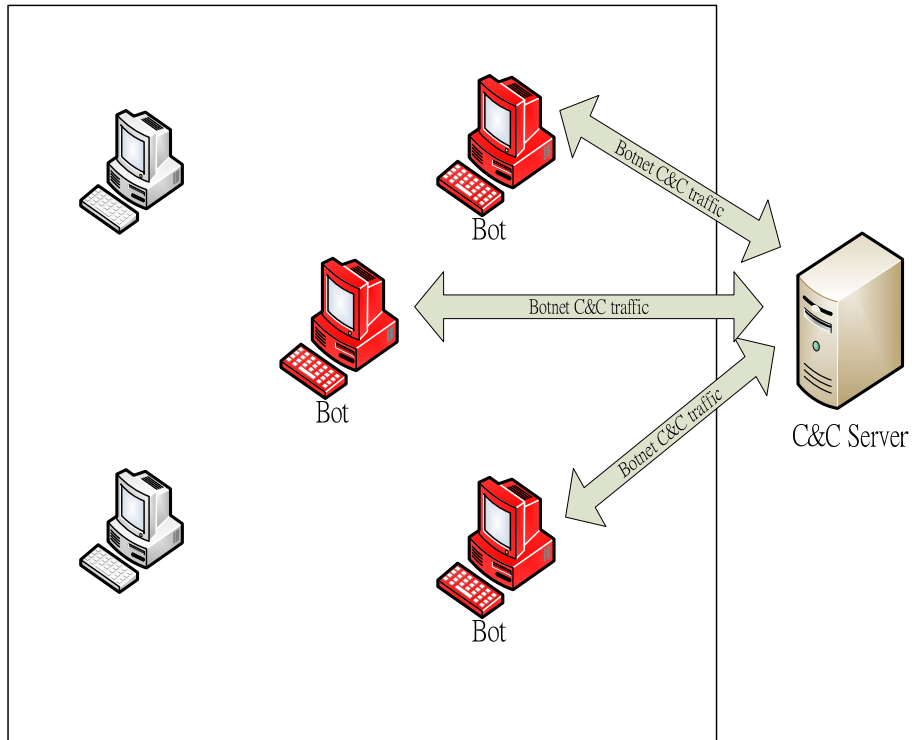


Figure 3: IRC Server is outside of LAN

In figure 3, because IRC server is outside of LAN, the proposed system can only detect the infected hosts and the IP address of IRC server which infected hosts connect. It helps network administrators find out the suspicious hosts and remove bot virus.

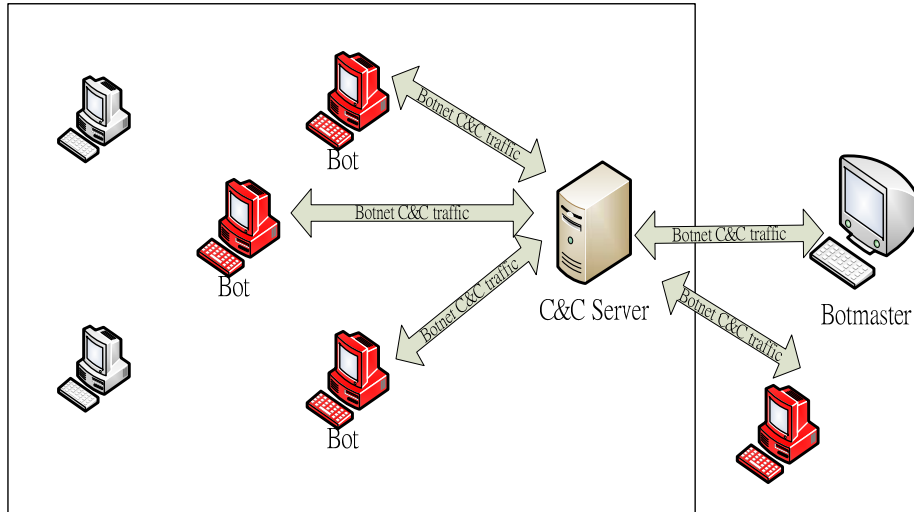


Figure 4: IRC Server is within LAN

In figure 4, because attackers might install an IRC server or use an existing IRC server as C&C server, C&C server is within LAN. Therefore, the proposed system can detect not only the infected hosts but also C&C servers. In this paper, we design a mechanism to find out suspicious hosts and IRC servers and we develop an on-line IRC IDS. To achieve this goal, there are four steps in the proposed system. Figure 5 illustrates the steps in the proposed system and the details of these steps will be described as following.

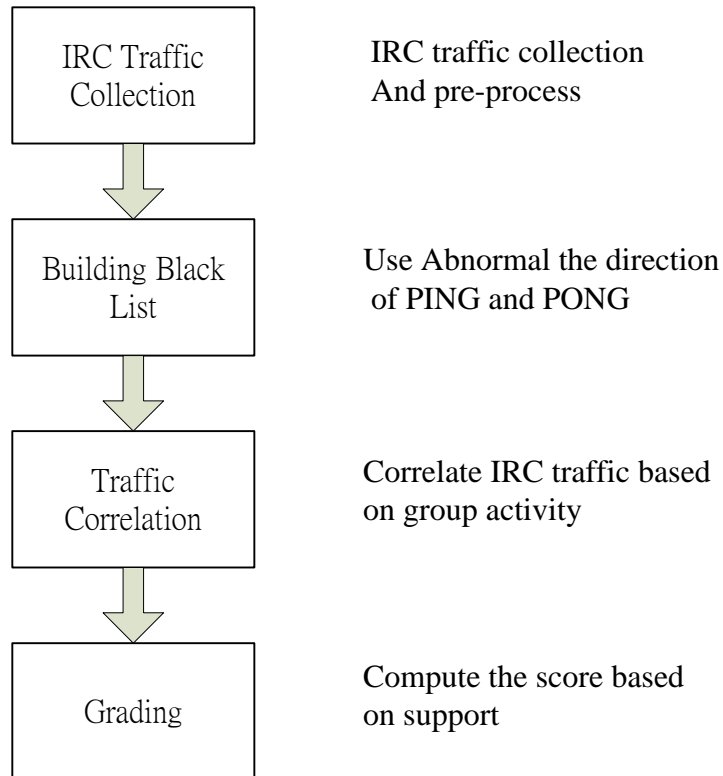


Figure 5. Processes of proposed system

Step 1:IRC traffic collection :

In step 1, we use two methods to collect the whole IRC traffic in LAN, they are IDS based approach and sniffer based approaches. In IDS based approach, we develop several IDS rules to collect IRC traffic. If there is already an IDS in LAN, IDS administrators can import these rules easily to collect IRC traffic. If there is no any IDS in LAN and network administrator do not want install a new IDS, a standalone IRC traffic logger is needed. Therefore, we develop an IRC traffic logger called IRC sniffer to collect whole IRC traffic in LAN. The features which we select are illustrated in table 1.

Table 1: Features of proposed system

Feature name	Description
Sip	Source IP address
Dip	Destination IP address
Sport	Source port
Dport	Destination port
Time	Timestamp of IRC traffic
Payload	Payload of IRC traffic

In this paper, the basic analysis unit is called record $R_i = \{ Sip, Dip, Sport, Dport, Time, Payload \}$, i stands for ID .

Step 2:Building Black List :

In this paper, we find an abnormal bot behavior called abnormal the direction of PING and PONG messages. If a host has this abnormal behavior, it must be a bot. Using this feature could help network administrators find infected hosts certainly and quickly. To avoid idle too long, some normal IRC client software would send a “PING” message to IRC server and IRC server would reply a “PONG” message to IRC client. Figure 6 illustrates the normal direction of “PING” and “PONG” message.

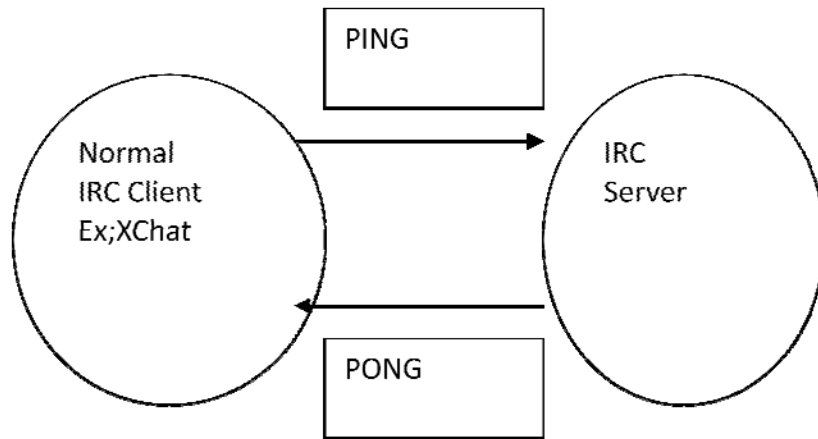


Figure 6: Normal direction of “PING” and “PONG” message

However, some bot hosts might not send “PING” messages to IRC servers periodically and automatically. Thus IRC server need to send a “PING” message to

IRC client when detects its clients are idle. If an IRC client receives a “PING” message from IRC server, it will response a “PONG” message to IRC server. Figure 7 illustrates the abnormal direction of “PING” and “PONG” message.

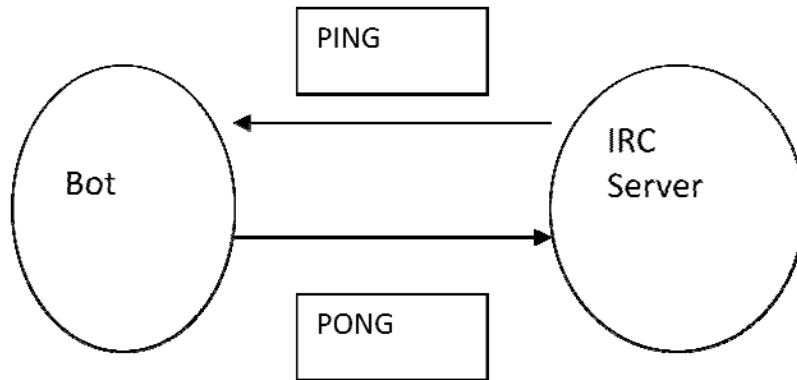


Figure 7: Abnormal direction of “PING” and “PONG” message

Step 3:Traffic Correlation :

Using abnormal direction of “PING” and “PONG” message can detect some type of Botnet. However, there are some bot viruses that do not have abnormal direction of “PING” and “PONG” message. Thus some detection approaches are needed. In this paper, we use group activity and homogeneous response to find suspicious hosts.

Group activity and homogeneous response in this paper mean a set of hosts receive a message from an IRC server and these hosts reply similar messages to the IRC server immediately at the same time. Figure 8 illustrates an example of a group.

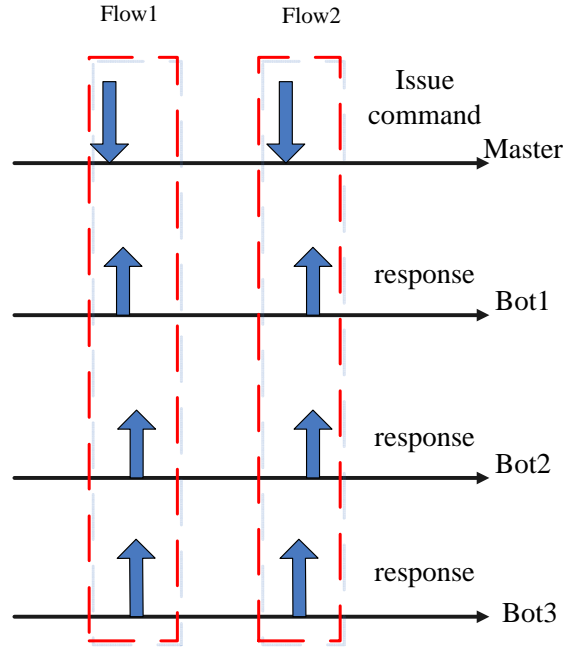


Figure 8: An example of a group

In figure 8, botmaster sends a command message to Bot1 Bot2 and Bot3 through an IRC server. Once Bot1 Bot2 and Bot3 receive this message, they will reply similar messages to IRC server. Thus we call Bot1 Bot2 and Bot3 are in a group.

There are two situations in Botnet attack in LAN. One is that botmaster installs an IRC server in LAN and uses it as C&C server, the other is the infected hosts are in LAN and connect to an external IRC server. In case 1, a group flow is defined in formula 1

$$G_{id}(R_c; R_1, \dots, R_n) = \begin{cases} 1 & \text{Sip}_i == \text{Dip}_j ; \text{Dip}_j \in \text{LAN} \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

In case 1, a group flow is defined in formula 2

$$G_{id}(R_c; R_1, \dots, R_n) = \begin{cases} 1 & \text{Sip}_c == \text{Dip}_j ; \text{Dip}_j \notin \text{LAN} \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

$G_{id}(R_c; R_1, \dots, R_n)$ means in a time slot, traffic $R_c, R_1, R_2, \dots, R_n$ are correlated as a group. R_c means the IRC traffic from IRC server and R_n means that the IRC traffic from suspicious hosts. In this paper, every time slot is ten seconds. In addition to group activity, homogeneous response is also an important feature. Homogeneous response means that all infected hosts could response similar messages to botmasters. In this paper, LCS (Longest Common Subsequence) is used to measure the similarity of messages. All client messages (R_n) in a group flow must follow homogeneous response feature. We set a threshold, once the LCS of these messages exceeds this threshold, we claim these messages follow homogeneous response feature. In step 3, several group flows are established. The proposed system will use them to identify infected hosts or internal C&C server.

Step 4: Grading :

In step 4, we will set a score to evaluate the risk of Botnet. The score is formed by correlation level of group flow and the confidence of a group. Correlation level of group flow means time difference between earliest and latest record of a group flow. The smaller of the time difference the higher of the correlation level. Figure 9 illustrates an example of correlation level.

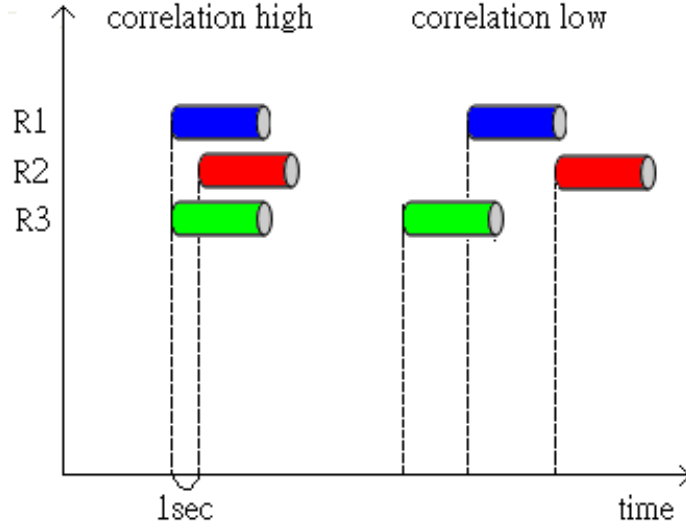


Figure 9: Example of correlation level

In this example, a group flow contain three records they are R_1 , R_2 and R_3 , we claim that the correlation level of left side group flow is high because time difference between earliest (R_1) and latest (R_3) record of a group flow is small. And the correlation level of right side group flow is low because time difference between earliest (R_1) and latest (R_3) record of a group flow is large. In this paper, we define three correlation levels and defined in formula 3.

$$C(Gid(R_c; R_1, \dots, R_n)) = \begin{cases} 1, & \text{if } Max(R_i) - Min(R_j) < 1; i \neq j \neq c \\ 0.9, & \text{if } 1 < Max(R_i) - Min(R_j) < 5; i \neq j \neq c \\ 0.8, & \text{if } 5 < Max(R_i) - Min(R_j) < 10; i \neq j \neq c \end{cases} \quad (3)$$

Formula 3 shows that if all hosts in this group response similar messages to an IRC server within 1 second, the correlation level is high and the value is 1. If all hosts in this group response similar messages to an IRC server between 1 to 5 seconds, the correlation level is medium and the value is 0.9. If all hosts in this group response similar messages to an IRC server between 5 to 10 seconds, the correlation level is low and the value is 0.8. We use correlation level as a measurement because in Botnet

command and control message transmission, infected hosts will response to botmaster immediately while receive the messages from botmaster. The high correlation level means all hosts send similar messages to the same IRC server at almost the same time. Therefore, the group flow with high correlation level might consist of Botnet command and control traffic.

If a group of hosts are compromised, they will communicate their botmaster frequently. Therefore, the proposed system could collect large volume of group flows, and vice versa. In this paper, we use group confidence to measure the likelihood of a Botnet group. Given a period of time, a set of hosts generate several group flows, $G_1(R_c; R_1, \dots, R_n), G_2(R_c; R_1, \dots, R_n) \dots, G_n(R_c; R_1, \dots, R_n)$, $|G|$ means the number of group flows that these hosts generate in the time period. The confidence of these

group is $conf = 1 - \frac{1}{e^{|G|} + 1}$.

And the score $S = \left(1 - \frac{1}{e^{|G|} + 1} \right) \times \prod_1^{|G|} C(G_{id}(R_c; R_1, \dots, R_n))$. In the proposed

system, if the score exceeds a threshold, the system will send an alert a system administrator. The default threshold in the proposed system is 0.63.

4 Experiments and Result

In this section, we illustrate the experimental result to validate the proposed system. The experimental environment is set up in testbed@ncku [5]. The network topology in testbed@ncku is illustrated in figure 10.

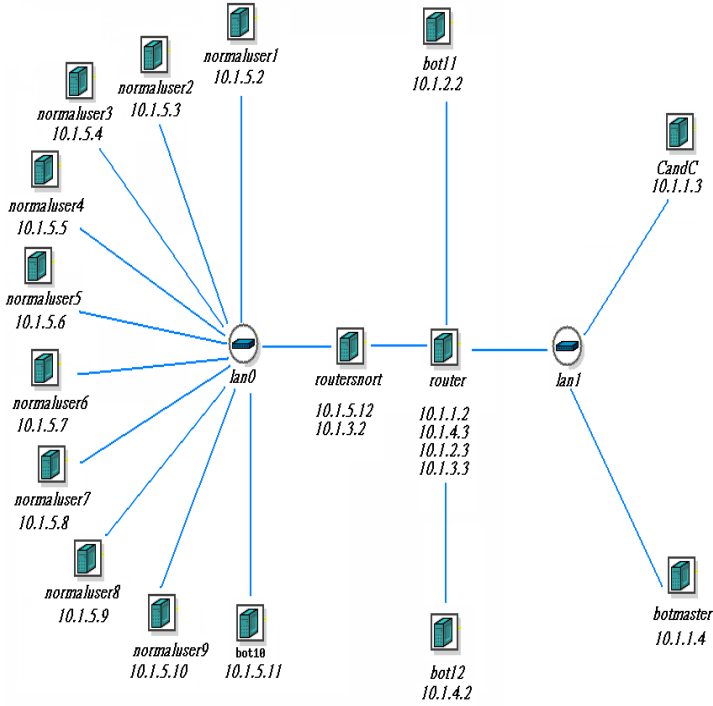


Figure 10: Network topology in testbed@ncku

There are two LANs in this experiment, the proposed system is installed in LAN0 and botmaster is in LAN1. There are one infected host in LAN0 and two infected hosts outside the LAN0. In this experiment, we want to observe if the volume of abnormal IRC traffic would affect the performance of proposed system. Thus we control the volume of abnormal IRC traffic to see the result. Table 2 and 3 illustrate the parameters in this experiment and table 4 illustrates the result.

Table 2: Environment setting in this experiment

Abnormal IRC traffic in LAN0	Number of infected host and normal hosts		Bots outside of LAN0
10%	9 normal user	1 bot	2 bot
50%	9 normal user	1 bot	2 bot
90%	9 normal user	1 bot	2 bot

Table 3 Number of messages in this experiment

Proportion	All Traffic	IRC Traffic	Correlation	After LCS
10%	380859	272861	5009	571
50%	385011	307151	1294	572
90%	390012	311359	779	521

Table 4 experimental result

False positive	False negative	True positive	True negative
0%	0%	100%	100%

Table 4 shows that the proposed system has excellent performance in all setting. The proposed system could detect all Botnet activities in LAN.

5 Conclusion and future work

In this paper, we use group activity, homogeneous response and abnormal the direction of PING and PONG messages to design an on-line intrusion detection system to detect abnormal IRC traffic in LAN. The experimental result shows that the proposed could detect all Botnet IRC traffic and identify the infected hosts. However, in this paper, we assume that attackers use only one IRC server and compromised hosts would never be turned off. In the future, the research will study that attackers use multiple C&C server and infected hosts are not stable (infected hosts might be turned off or re-install OS or botmaster remove the virus after attack is completed).

6 Reference

1. H. Choi, H.Lee, H. Lee, H. Kim, Botnet Detection by Monitoring Group Activities in DNS Traffic,7th IEEE International Conference on Computer and Information Technology (CIT 2007), 2007.
2. G. Gu, J.Zhang, and W. Lee, BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic, 15th Annual Network & Distributed System Security Symposium, 2008
3. S. Ji, C.Im, M. Kim, H. Jeong, "Botnet Detection and Response Architecture for Offering Secure Internet Services," 2008 International Conference on Security Technology, pp.101-104,2008
4. K.Takemori,Y. Miyake, C. Ishida, I.Sasase,A SOC Framework for ISP Federation and

18 **Gu-Hsin Lai** , Chia-Mei Chen¹, and Ray-Yu Tzeng², Chi-Sung Lai², Christos Faloutsos³

Attack Forecast by Learning Propagation Patterns, *Intelligence and Security Informatics*, Vol.23, No.24, pp.172 - 179,2007

5. Testbed@ncku, <http://testbed.ncku.edu.tw>

6. R. Villamarín-Salomón and J. Carlos Brustoloni, Bayesian bot detection based on DNS traffic similarity, *Proceedings of the 2009 ACM symposium on Applied Computing*, 2009,p.p 2035-2041

7. A. Wald. *Sequential Analysis*. Dover Publications, 2004