Bots Behaviors vs. Human Behaviors on Large-Scale Communication Networks (Extended Abstract)

Wei Lu[1,2] and Ali A. Ghorbani[1]

[1] Faculty of Computer Science, University of New Brunswick, Fredericton,
NB Canada
[2] Department of Electrical and Computer Engineering, University of Victoria,
BC Canada
{wlu,ghorbani}@unb.ca

Abstract. In this paper we propose a hierarchical framework for detecting and characterizing any types of botnets on a large-scale WiFi ISP network. In particular, we first analyze and classify the network traffic into different applications by using payload signatures and the cross-associations for IP addresses and ports. Then based on specific application community (e.g. IRC, HTTP, or Peer-to-Peer), we present a novel temporal-frequent characteristic of flows that leads the differentiation of malicious behaviors created by bots from normal network traffic generated by human beings. We evaluate our approach with over 160 million flows collected over five consecutive days on a large-scale network and preliminary results show the proposed approach successfully detects the IRC botnet flows from over 160 million flows with a high detection rate and an acceptable low false alarm rate.

1 Problem Statement, State of the Art and Contributions

Detecting botnets behaviors on large-scale networks is a very challenging problem. This is because: (1) botnets are often hidden in existing applications, and thus their traffic volume is not that big and is very similar with normal traffic behaviors; (2) identifying network traffic into different applications becomes more challenging and is still an issue yet to be solved due to traffic content encryption and the unreliable destination port labeling method. The observation on a large-scale WiFi ISP network over a half year period showed that even exploring the flow content examination method, there are still about 40% network flows that cannot be classified into specific applications. Investigating such a huge number of unknown traffic is very important since they might stand for the abnormalities in the traffic, malicious behaviors or simply the identification of novel applications.

Current attempts on detecting botnets are mainly based on honeypots, passive anomaly analysis and traffic application classification. The anomaly analysis for detecting botnets on network traffic is usually independent of the traffic content and has the potential to find different types of botnets. However, anomaly

R. Lippmann, E. Kirda, and A. Trachtenberg (Eds.): RAID 2008, LNCS 5230, pp. 415–416, 2008.

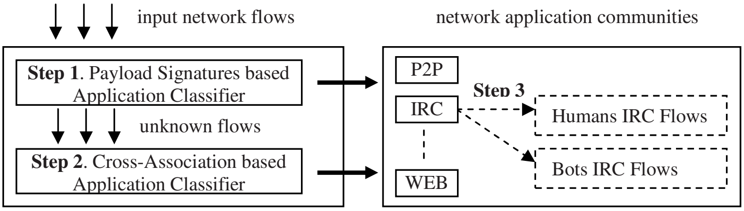
input network flows
Step 1. Payload Signatures based Application Classifier
unknown flows
Step 2. Cross-Association based Application Classifier
network application communities
P2P
IRC
WEB
Step 3
Humans IRC Flows
Bots IRC Flows

Fig. 1. The proposed hierarchical framework for botnets detection

detection tends to generate a large volume of false alarms traditionally when deployed on a large-scale communication network. The traffic application classification based botnets detection focuses on classifying traffic into IRC traffic and non-IRC traffic, offering a potential to reduce number of false alarms, but can detect IRC based botnets only.

In this paper, we focus on traffic classification based botnets detection. Instead of labeling and filtering traffic into non-IRC and IRC, we propose a hierarchical framework illustrated in Fig. 1 for discriminating malicious behaviors generated by any types of bots from normal behaviors generated by human beings. The major contributions of this work include: (1) a novel application discovery approach for classifying traffic into different network application communities (e.g. P2P, Chat, Web, etc.) on a large-scale WiFi ISP network, in which the input flows are first labeled through payload signatures (i.e. Step 1 of Fig.1) and unknown flows are then labeled through the cross-associations of IP addresses and port numbers (i.e. Step 2 of Fig.1); (2) a novel temporal-frequent metric based on N-gram (frequent characteristic) of flow payload over a time period (temporal characteristic) for discriminating bots behaviors from humans behaviors on a large-scale network (i.e. Step 3 of Fig.1).

2 Preliminary Evaluation Results and Conclusions

We implement a prototype system for the proposed hierarchical framework and then evaluate it on a large-scale WiFi ISP network over five consecutive business days. Our traffic classification approach can classify the unknown IRC flows into the IRC application community with a 100% classification rate on the five days evaluation. The detection rate for differentiating bots IRC traffic from normal human beings IRC traffic is 100% on four days testing, while an exception happens on the third day's testing on which our prototype obtained a 77.8% detection rate with a 3.1% false alarm rate. The best evaluation over the five days testing is a 100% detection rate with only 1.6% false alarm rate. Moreover, the preliminary evaluation results show that the average standard deviation of bytes frequency over the 256 ASCIIs on the flow payload is an important metric to indicate normal human IRC traffic and malicious IRC traffic generated by machine bots. In the near future, we will conduct an experimental evaluation with the web based botnets and new appeared P2P botnets.