Proceedings of Engineering and Technology Innovation, vol. 3, 2016, pp. 28 - 30

Using Unsupervised Machine Learning to Detect Peer-to-Peer Botnet Flows

Andrea E. Medina Paredes[1], Yuan-Yuan Su[2], Wei Wu[3], Hung-Min Sun[4,*]

[1]Institute of Information Systems and Applications, National Tsing Hua University, Hsinchu, Taiwan.

[2]Department of Computer Science, National Tsing Hua University, Hsinchu, Taiwan.

[3]Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, Fujian, China.

[4]Department of Computer Science, National Tsing Hua University, Hsinchu, Taiwan.

Received 22 February 2016; received in revised form 19 March 2016; accepted 06 April 2016

Abstract

The war against botnet infection is fought every day by users that want to feel safe against any threat of compromise hosts. In this paper we are going to focus on the behavior of Peer 2 Peer (P2P) botnets, which along with hybrid botnets is a growing trend among attackers. The main approach will consist of a behavior comparison among features extracted from network flows, focusing only in the flows from P2P applications including P2P botnets.

Keywords: clusters, network flows, P2P botnets, unsupervised learning

1. Introduction

Malicious software such as botnets has been around for quite a time already and it keeps improving, evolving and growing, as for the detection systems, they try to keep track of these new emerging botnets trends but some fail to provide a definite and accurate solution to this problem. For example, this past May “8chan”, a website composed of user-created boards, reported a series of DDoS attacks coming from the “Hola!” network, a popular virtual private network use for viewing blocked videos and TV shows from other countries, which counts with a pool of 6 million IP addresses [1].

Activities such as adding signatures to databases, protecting servers against hackers, the use anti-virus software to protect computers from getting infected, track C&C server activities and so many other actions are taken in consideration, but still cybercriminals find a way to go around the security measures. The use of supervised learning models is one of many approaches that can be use to deal with botnets, classifiers like support vector machines (SVM) have shown great accuracy separating botnet network flows from normal flows [2], other methods like decision tree algorithms have been put to the test as well, measuring how accurate the decision tree classifies the data [3]. The drawback of the previous mention methods is that most of them need labelled data in order to function and only yields better results when the botnet signature is already known.

In hopes to contribute to these efforts, in this paper we propose the use of Unsupervised Machine Learning algorithms for the fight against botnet detection. A comparison among three clustering algorithms using network flows extracted from a set of features, will be carried out thorough out this paper. The rest of this paper, is organized with the following: the method use, the experiment design with the respective observations and finally the analysis of the results.

2. Method

The structural synthesis of CCPGTs will be performed based on the creative design methodology process [7-8].

The design requirements and design constraints are summarized based on the characteristics of the mechanism.

2.1. Approach using Unsupervised Learning

Traffic can be classified by selecting its at-

* Corresponding author. Email: hmsun@cs.nthu.edu.tw

tributes which distinguishes their behavior, we want the unsupervised learning algorithm to find the patterns hidden among the P2P flows. To facilitate the algorithm detection a previous process to select the most relevant features will be carry out and then these input will be feed to the clustering algorithms in order to compare their overall performance creating clusters based on the characteristics of those features. Then the resulting cluster will be cross validated in order to ensure the legitimacy of the outputs. Fig. 1 shows a flowchart with the overall process:

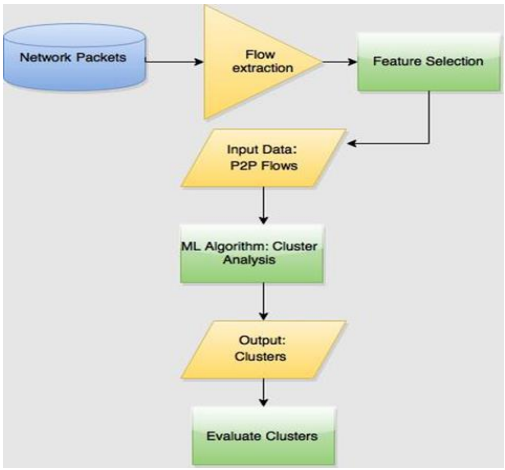

Fig. 1 Overall process of the approach using Unsupervised Learning

2.2. Clusters Evaluation Measurements

In this paper we choose Simple K-means, Farthest First [4] and DB Scan [5] to work with clustering algorithms to compare which is the best fit to classify P2P botnets traces using network flows extracted from the packets send within a network [6].The data is divided later into subsets for evaluating the machine learning algorithms, the sets contain P2P traffic from both kind's malicious flows and Non- Malicious flows. Performance statistics are calculated for all the trials. The class is ignored during all the evaluations for the clusters. The validation measures are used to evaluate the credibility of the clusters, in this case due to the high imbalance between classes, to keep the real scenario of a network, we can't only rely on the accuracy measurement of the clusters.

The Classification Oriented Measures of Cluster Validity are described below:

- The number of correctly classified instances as malicious is referred to as the True Positive (TP).
- The number of instances classified as malicious but should be normal and therefore rejected, is referred to as the False Positive (FP).
- The number of instances classified as normal but are actually malicious, is referred to as the False Negative (FN).
- The number of normal instances from a class correctly rejected is referred to as True Negative (TN).

3. Results and Discussion

We need to utilize clustering algorithms which can handle such differences in the data along with the first 10 top ranked attributes from the feature extraction. As mention before we used WEKA [6] to run this three clusters.

3.1. Dataset Assemble for Testing

The dataset used in this paper was obtained from a previous research group that made the datasets publicly available, their paper is about a P2P traffic categorization system called "Peer Rush" [8]. The labeled data of all four P2P applications (Emule, UTorrent, Vuze and FrostWire) along with Zeus and Waledac were used for testing purposes. The dataset was divided into 3 combinations of subsets, containing both kinds of flows that are labeled either Non-Malicious or Malicious:

- **Dataset 1** (Zeus traces)**:** A total of 17,940 flows are contained in the dataset, 95% non-malicious traces and 5% malicious traces.
- **Dataset 2** (Waledac Traces): A total of 12,310 flows are contained in the dataset, 93% non-malicious traces and 7% malicious traces.
- **Dataset 3** (Zeus and Waledac traces): A total of 12,334 flows are contained in the dataset, 92% non-malicious traces and 8% malicious traces.

3.2. Unsupervised Learning Comparison

The accuracy of all the algorithms is shown in Fig. 2.

DB Scan performed significantly well for all the situations assigned, each change of dataset diminishes slightly the accuracy, but in general it maintains the highest percentage. Simple

K-means improved in the last test but still had some imbalance in the number of correctly classified malicious instances that were retrieved.

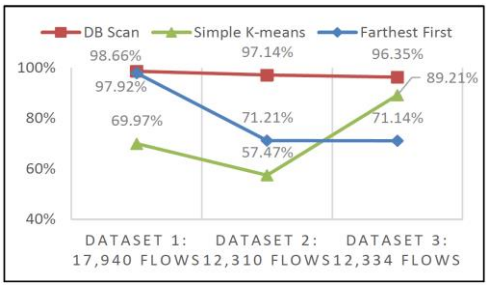

Fig. 2 Accuracy of Unsupervised Algorithms for all Datasets

In Table 1 we can compare the real performance values of each algorithm. DB Scan proves to be a worthy contender against P2P botnets flows and may be used to improve the precision of detection systems along with other security tools. We believe that each algorithm performs depending on the quality of the data and the previous preprocessing of it.

Table 1 Average measurement values for each algorithm

Algorithms	Average Accuracy	Average Precision	Average Recall	Average F-measure
Farthest First	80.09%	0.2763	0.4588	0.3378
DB Scan	97.38%	0.9592	0.6723	0.7857
Simple K-means	72.22%	0.2364	0.9463	0.3621

4. Conclusions

The use of unsupervised learning was proposing for classifying P2P traffic flows in comparison to the previous methods using supervised learning. The results lead us to believe the data is suitable for a density based cluster, since DB Scan algorithm performed well on every situation, obtaining high precision classifying P2P botnet flows and retrieving most of these malicious flows from the normal P2P Traffic.

Acknowledgement

This research was supported in part by the Ministry of Science and Technology, Taiwan, under the Grants MOST 104-3115-E-007-004 and MOST 103-2221-E-007-073-MY3.

References

[1] R. Price, "Business Insider," http://www.businessinsider.com/hola-used-for-botnet-on-chrome, May 2015.

[2] P. Barthakur, M. Dahal, and M. K. Ghose, "A framework for P2P botnet detection using SVM," in International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover, Sanya, 2012.

[3] W. H. Liao and C. C. Chang, "Peer to peer botnet detection using data mining scheme," International Conference on Internet Technology and Applications, Wuhan, 2010.

[4] S. Hochbaum, "A best possible heuristic for the k-center problem," in Mathematics of Operations Research, 1985.

[5] P. N. Tan, M. Steinbach, and V. Kumar, "Cluster analysis: basic concepts and algorithms," Introduction to Data Mining, Pearson, pp. 487-559, 2005.

[6] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The WEKA data mining software: an update," SIGKDD Explorations, 2009.

[7] B. Rahbarinia, R. Perdisci, A. Lanzi, and K. Li, "PeerRush: mining for unwanted P2P traffic," Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, vol. 7967, pp. 62-82, 2013.