International Journal of Technology and Engineering System (IJTES)
Vol 7. No.5 2015 Pp. 442-444
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

Efficient Detection Technique to Detect Known and Unknown Traffic WORM

K. Archana[1], Dr. R. Indra Gandhi[2]
[1]PG Research Scholar, [2]Head of the Department
[1,2]Department of Master of Computer Applications
GKM College of Engineering and Technology, Chennai
[1] archanamalavika@gmail.com , [2]shambhavi.rajesh@gmail.com

ABSTRACT

Security has become ubiquitous in every area of malware newly emerging today pose a growing threat from ever perilous systems. As a result to that, Worms are in the upper part of the malware threats attacking the computer system despite the evolution of the worm detection techniques. Several recent researches in the few last years were proposed and presented towards "Worms Detection" domain based on data mining as an efficient ways to increase the security of networks. Classification technique was the best for many resent researches. Existing model support for detecting unknown worms and it is used to identify worm traffic from normal traffic. The proposed system uses ANN for classifying worm/ non worm traffic with accuracy of 99%, and predicting the percentage of infection in the infected network with absolute error average from 0% to 4%, which can be used by the administrator to take the right action. Proposed Worm detection schemes that are based on the global scan traffic monitor by detecting traffic anomalous behavior, there are other worm detection and defense schemes such as sequential hypothesis testing for detecting worm-infected computers, payload-based worm signature detection.

Keywords : Threat, Detection, worm traffic, Classification, Network Security.

I. Introduction

The few systems that attempt to detect unknown worms attacks are usually crippled by other factors such as the amount of traffics. Automatic detection is particularly challenging because it is difficult to predict what form the next worm will take so, an automatic detection and response is rapidly becoming an imperative because a newly released worm can infect millions of hosts in a matter of seconds. Several different types of machine learning techniques were used in the field of intrusion detection in general and worm detection in particular. Data Mining has an important role and is essential in worms detection systems, which using different data mining techniques to build several models have been proposed to detect worms. Worms are divided in two different kinds' direct worms, which don't need a medium to propagate, because they use computer networks, exploiting operating systems bugs or weaknesses. The worm's life consists of four phases: target finding, which was the first step in a worm's life to discover vulnerable hosts, transferring that refers to sending a copy of the worm to the target after the target is discovered, activation is when a worm starts performing its malicious activities. The activities in the two latter phases are limited to local machines and are harder to detect by NIDSs. The first two phases cause network activities, worm behaviours in these two phases

are critical for developing detection Algorithms. In this paper we focus on direct worms.

II. Literature Review

Detecting worms mining dynamic program execution by Xun Wang et al[1] describes Worm attacks have been major security threats to the Internet. Authors propose a new worm detection approach based on mining dynamic program executions. To detect new worms in terms of a very high detection rate and a low false positive rate.

Detecting Internet Worms Using Data Mining Techniques by Muazzam siddiqui et al [2] attempted traditional approaches using signatures to detect worms pose little danger to the zero day attacks. This Approach showed 95.6% detection rate on novel worms whose data was not used in the model building process the focus of malware.

Detection of Unknown Computer Worms Activity by Robert Moskovitch et al [3], expressed as detection of unknown worms is a challenging task. Extant solutions, such as anti-virus tools, rely mainly on prior explicit knowledge of specific worm signatures. As a result, after the appearance of a new worm on the Web there is a significant delay until an update carrying the worm's signature is distributed to anti-virus tools. An innovative technique for detecting the presence of an *unknown* worm, not necessarily by recognizing specific instances of the worm, but rather based on the computer measurements.

Intelligent System for Worm Detection by A.Farag et al [4]describes Worms are on the top of malware threats attacking computer system although of the evolution of worms detection techniques. Early detection of unknown worms is still a problem. The proposed system uses Artificial Neural Network (ANN) for classifying worm/ non worm traffic and predicting the percentage of infection in the infected network.

A Malware Detection Scheme Based on Mining Format Information by Jinrong Bai et al[5]expressed Malware has become one of the most serious threats to computer information system and the current malware detection technology still has very significant limitations. In this paper, we proposed a malware detection is approach by mining format information of PE (portable executable) files.

III. Implementation

Step 1: Building "WDMAC" Model

To build "WDMAC" model which is an adaptive worm's detection model based on multi classifiers that able to detect known and unknown worms, we have conducted the following steps:

Step 1.1: The Base Line Experiments : To select the classifiers will be used in building the "WDMAC" model, we make 3 groups of datasets samples, and apply the six commonly algorithms of classifier which are: Support Vector Machines (SVM), Rule Induction (RI),K-Nearest Neighbor (K-NN), Naïve Bayes (NB), Decision Tree (DT), and Artificial Neural Network (ANN).

Step 2: K-Nearest Neighbor (K-NN) algorithm achieved the highest results of Naive Bayes algorithm, but there is another factor to be taken into consideration, which is the results of NB in case 3 (unknown worm detection) was best of K-NN, where the case 3 of experiments consider the important case that was the natural case of worms detection.

Step 3: Support Vector Machine (SVM) algorithm has been excluded because the results are not good compared with other algorithms used in thi phase.

Step 4: Rule Induction (RI) algorithm was excluded also, because the result is not good compared with other algorithms used in this phase.

Step 5: So, the selection of suitable algorithm use in "WDMAC" model as follows: Naïve Bayes (NB) algorithm, Decision Tree (DT) algorithm, and Artificial Neural Network (ANN), where achieved the balancing between three factors

Step 6: Evaluate the "WDMAC" model

The following are four definitions of the members of the matrix: the True Positive rate (TP), False Positive rate (FP), True Negative rate (TN), False Negative rate (FN). Also, accuracy considered the most commonly to evaluate classification performance.

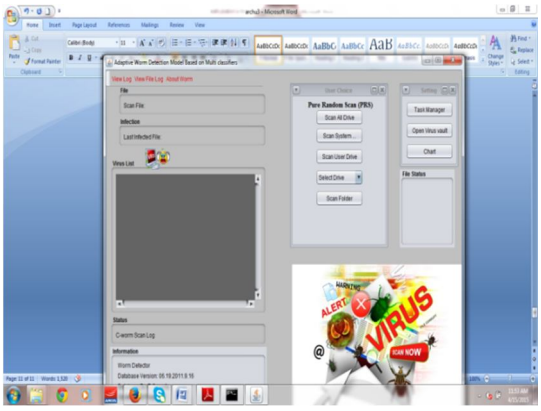

Figure 1: Opening Screen for worm detection

scan all drive button is use to scan all the drives such as C,D,E and we also use select drive button to scan the particular drive by selecting it. Scan system is to scan and detect the virus in the system. Scan folder is to scan and detect the particular folder

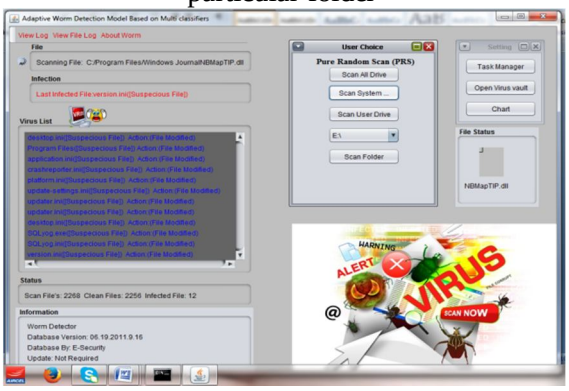

Figure 2: Detection of Virus List

By selecting the E:/ drive the list of viruses will be displayed on the particular dialog box

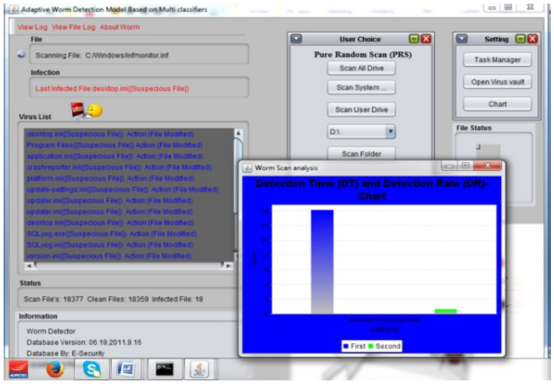

Figure 3: Worm Scan Analysis Chart

By clicking the chart button, the chart will display with detection time (DT) and detection rate (DR).

IV. conclusion

In our research, we present three efficient classification techniques in data mining, which are Naïve Bayes (NB), Decision Tree (DT), and Artificial Neural Network (ANN). These techniques were used in applying “WDMAC” model. We proposed "WDMAC" which is an adaptive model based on multi classification that able to be detecting known and unknown worms.

The purpose of used multi classification was to obtain the highest accuracy and detection rates, and reduced misclassification rates. Our results show that the proposed model has achieved higher accuracies and detection rates of classification, where detection known worms are at least 98.30%, with classification error rate 1.70%, while the unknown worm detection rate is about 97.99%, with classification error rate 2.01%.

V. Reference

1. Stopel, D.; Boger, Z.; Moskovitch, R.; Shahar, Y.;and Elovici, Y.; “Application of Artificial Neural Networks Techniques to Computer Worm Detection”, International Conference on Neural Networks ICNN International Journal of Applied Mathematics and Computer Sciences,2006.
2. Pietro R.; and Mancini L.; “Intrusion Detection Systems”, Springer Science and Business Media, LLC., 2008.
3. Li P., Salour M., and Su X., "A Survey of Internet Worm Detection and Containment". Communications Surveys & Tutorials, IEEE, 2008.
4. Douligeris Ch.; and Serpanos D.; “Network Security Current Status and Future Directions”, IEEE Press, 2007.
5. Farag, A.; Shouman, A.; Sobh, S.; and El-Fiqi, Z.;,"Intelligent System for Worm Detection", International Arab Journal of e-Technology, Vol.1, No. 1, January 2009.