International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Analysis of Botnet Domain Names for IoT Cyber Security

Prof. Sheetal Mungale, Akshata Chokhandre, Prerna Namulwar, Neha Raut, Aparna Meshram

Electronic and Telecommunication Engineering,

S.B Jain Institute of Technology Management and Research,

Nagpur-441501, Maharashtra, India

Abstract

A botnet is a network of take over computers and devices infected with bot malware and remotely controlled by a hacker. The rapid development of the internet of things(IOT) applications the botnet can easily make use to IOT devices for large-scale attacks.Botnets are network of hijacked computer devices use to carry out various scams and cyber attacks.The term “Botnet” is formed from two words robot and network. Robot means an automatic program run and perform the intended task without user interaction.Botnet is a program able to scan any network using Router.Router can identify or scan log (packets) by using malware detection.the IoT devices are always not be installed with sophisticated software to defense the botnet, and on other way, the IoT devices are not always updated in time and then the vulnerabilities or bugs can be easily used by the botnet. generally, the bot or robot generates a series of domain names based on an algorithm and it can dynamically updates the location of C&C(command and Control) server with shifting the active DNS entry.Then the bots can always request the active domain name to access the Command and control server to listen to the command even when the C&C server changed its location.

Keywords: IoT botnet, security machine learning,clustering

1.Introduction

Botnet are set of devices (i.e, computers) which are Identified for specific malware software and then these devices can be remotely controlled to launch large-scale malware attacks Malware software is any program or file that is intentionally harmful to a computer, network or server.For example. With the rapid development and wide deployment of the Internet of Things (IoT), more insecure devices will be connected into the public Internet and they can be easily controlled by the botnet. Then IoT based botnet becomes one of the biggest security issues in the future Internet.Identify Logs Protocol,Types of packets,size of packets,port number and then scan for malware detection.

2.Literature Survey

paper[Analysis of Botnet Domain Names for IoT Cybersecurity]The Researcher discuss deploy this model under larger DNS data size and use more sophisticated learning algorithms to detect the malicious domain names for protecting critical infrastructure.we focus on the deep analysis of the botnet domain name characteristics and then try to detect the botnet domain names efficiently and accurately. In such a way,the botnet domain names can be separated out and the determined can be immediately to stop. And the work in this paper is an extension based on our previous achievement with extended feature analysis

and expanded dataset in order to demonstrate the effectiveness of these characteristic and determine the botnet domain name more advantages.

paper[Efficient Detection of Botnet Traffic by features selection and Decision Trees]The researcher describe the most relevant features using the Gini Importance and Information Gain criteria.The Gini Gain is defined as the variation of the Gini Impurity after a split of the data using a feature.Information Gain allows us to quantify which fea-ture provides maximal information about the classification, using for that the notion of entropy. The Information Gain obtained with a characteristics is defined as reducing the entropy in the dataset after knowing the values of the samples for this feature.

paper[Botnet Detection Technology Based on DNS]In this paper Gaining the attention of attackers, it is vulnerable to attack.This paper focuses on evasion and detection techniques of DNS-based botnets and gives a review of this field for a summary of all these contributions. Some important topics, including technological background, evasion and detection, and alleviation of botnets, ar discuss.

paper[Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research]This paper briefly investigate Machine Learning (ML) algorithm and effective features.Thus, this study aimed to identify, assess and provide a thoroughly review of experimental works on the research relevant to the detection of IoT botnets.The authors analyzed the nominated research and the key methods related to them. The detection methods have been classified based on the techniques used, and the authors investigated the botne phases during which detection is accomplished.

paper[Survey on Botnet Detection Techniques]The author explain the introduces the new construction mechanism of botnet.*is survey analyzes and compares the most important efforts in the botnet detection area in recent years. It studies the characteristics of botnet architecture, life cycle, and command and control channel and provides a classification of botnet detection techniques It focuses on the application of advanced technologies such as deep learning, complex network moving target defense

(MTD), and software-defined network (SDN) for botnet detection.

3.Working

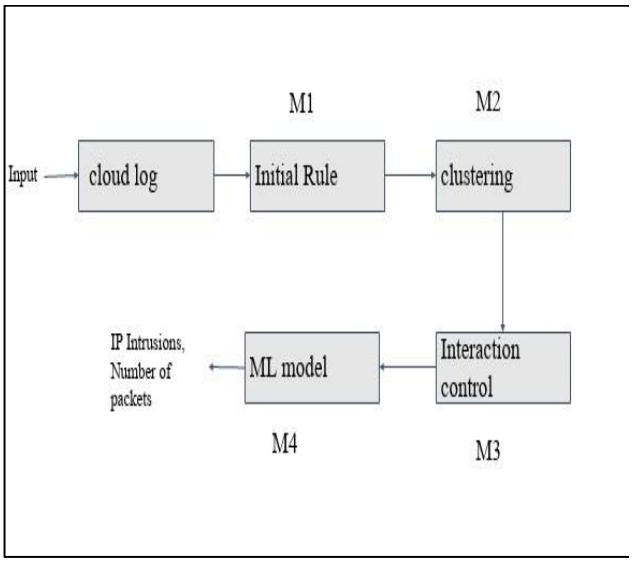


Figure 1. Flow diagram of the proposed Bot Net Model system

Cloud log - Cloud log is a fully managed service that allows you to store,search,analyze, monitor and alert on logging data and events from google cloud.

Initial rules - Check port size, ip address,port number.

Clustering - Clustering is to remove unwanted entries and classification is to identify which entries are malware.

Instruction control - They are used for clustering.

ML model - They are used for classification.

There are four module initial rules, clustering, interaction control , ML model. Input from cloud logs and then send to initial rule.

Initial rule is use to check the packet size or port number. packet size is the range of 20 to 5000 then it is identify as.System with less than 200 port if the user is using this less it means its malware.Clustering is to remove unwanted entries and classification is to identify which entries are malicious.

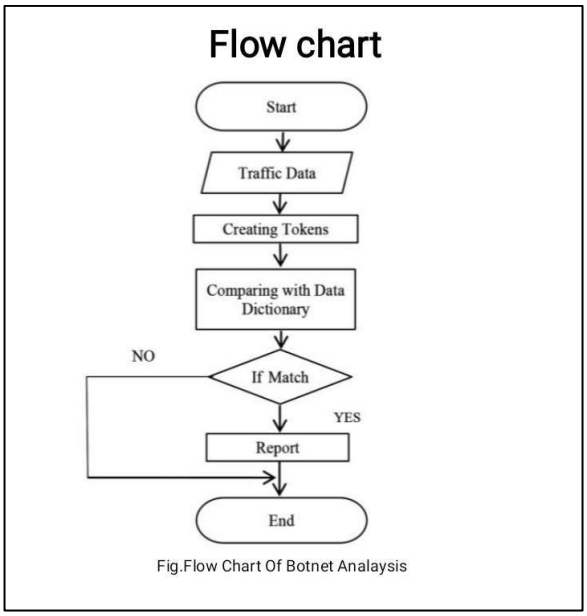


Fig.Flow Chart Of Botnet Analaysis

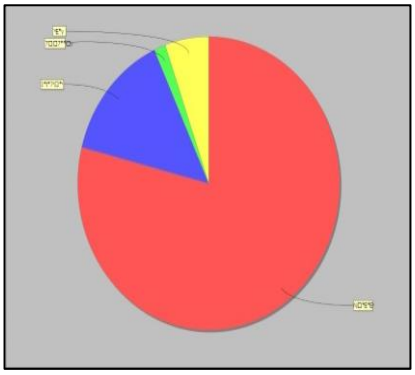
4.Software

Language- Java, Software- Eclipse

Eclipse-Eclipse is an combine development environment used in computer programming. It contains a base workspace and an extendable plug-in system for modifying the environment. It is the second-most-popular

IDE for Java development, and, until 2016, was the most popular.Eclipse is a free, Java-based development platform known for its plugins that allow developers to established and test code written in other programming languages. Eclipse is to be free under the terms of the Eclipse Public License.

5.System Graph



6. Results and Conclusion

It provides key platform for many cyber crimes.Botnet Pose Significant and growing threat against cybersecurity.It is very important to detect botnet attack and find the solution for it.Its shows normal IPs and IPs attack.It shows which IP address is attack under the Iot.Graph shows how many normal Ips, attacks and accuracy.There is no doubt that the Internet of Things is conducive to social development and civilized progress, and its security threats come from our needs for smart homes, smart cities, and industrial automation. Only by handling all security-related issues in the Internet of Things can the vision of the Internet of Everything become a reality.

Blue Color Shows-normal IP.
Red Color Shows-attack IP.
Yellow Color Shows-Delay.
Green Color Shows-Accuracy.

7. References

[1] WANTING LI1,JIAN JIN1"Analysis of Botnet Domain Names for IoT Cybersecurity under the ITRC (Information Technology Research Center),2017.

[2] Velasco-Mata, Javier,"Efficient Detection of Botnet Traffic by features selection and Decision Trees".Researcher at INCIBE, León (Spain),2021.

[3]Xingguo Li1, Junfeng Wang,"Botnet Detection Technology Based on DNS".National Key Laboratory of Fundamental Science on Synthetic Vision,2017.

[4] Majda Wazzan 1, Daniyal Algazzawi,"Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research". Computer Science Department, Faculty of Computing and Information Technology,2021.

[5] Dannong Li,3 and Li Guo2,"Survey on Botnet Detection Techniques".Teaching and Research Support Center,2021.