International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 03 Issue: 01 | Jan-2016 www.irjet.net p-ISSN: 2395-0072

A Survey of HTTP Botnet Detection

Saurabh P. Chaware [1], Prof. Sukhada Bhingarkar[2]

[1] *Department of Computer Engineering, MIT COE,Pune, Maharashtra, India.*
[2] *Department of Computer Engineering, MIT COE,Pune, Maharashtra, India.*

Abstract - ***A botnet is a group of cooperated computers which are remotely controlled by hackers to launch various network attacks, such as DDoS attack, junk mail, click fraud, individuality theft and information phishing. The recent botnets have initiated using common protocols such as HTTP which makes it even harder to distinguish their communication patterns. Most of the HTTP bot transportations are founded on TCP connections. Of all current threats to cyber security, botnets are at the topmost of the list. In importance, attention in this problem is increasing rapidly among the research community and the number of journals on the question has grown-up exponentially in recent years. This article proposes a survey of botnet research and presents a survey of botnet detection***.

Key Words: *Botnet, Feature Extraction, Feature Reduction, Legitimate user.*

1. INTRODUCTION

Botnets are one of the most thoughtful current dangers to cyber security. The term botnet is used to define a network of infested machines, termed bots, which are below the control of a human operator commonly known as the bot master. Bots are used to carry out a inclusive variability of mischievous and harmful actions against systems and services, including denial-of-service (DoS) attacks, spam spreading, phishing, and click fraud. Botnets are organized networks of infected (Zombie) machines running bot codes, categorized by their use of a command and control (C&C) channel. Using the command and control of botnet, a bot master can control a large group of compromised bots and then perform malicious attacks . At early times, C&C communications were based on Internet Relay Chat (IRC) protocol. The attacker used to actively issue commands on the special channel of IRC server to all the bots. Recently, HTTP becomes a more popular communication protocol for bots. These web-based C&C bots try to mixture into regular HTTP traffic, which makes them more difficult to be identified, since HTTP is a commonly used network communication protocol in many applications. The HTTP bots frequently demand and download instructions from web servers under the attacker's control. As a result, detecting bots with web-based controlling is more intricate than bots with IRC-based controlling.

In this study, we have encountered various techniques for HTTP botnet detection and methodologies used in them.

2. LITERATURE SURVEY

2.1 HTTP Botnet Detection Using Adaptive Learning Rate Multilayer Feed-Forward Neural Network

In this paper, author proposed a new method to identify HTTP-based botnet by using the network behavior of botnet. On observation of activities of web-based botnet, Author also noticed that most of the communications of web-based botnets are based on TCP connections, so author extracted the TCP connection behavior shared by web-based botnets used it as features and create a neural network model which detect the HTTP botnet traffic.

2.1.1Methodology Used:

In this work firstly some TCP related features have been extracted for the detection of HTTP botnets. Extracted features is used to built a Multi-Layer Feed Forward Neural Network training model using Bold Driver Back-propagation learning algorithm.

2.2 Http Botnet Detection Using Frequent Patternset Mining

In proposed detection technique, incoming and outgoing network traffic is monitored then network traffic filtering and separation is done. Apriori algorithm is used for frequent patternset generation with use of timestamp.

Author believes that Data mining algorithms helps to automate detecting characteristics from large amount of data, on which the conventional heuristics and signature based methods could not apply. In this paper author proposed HTTP botnet detection technique by combining data mining technique and timestamp.

2.2.1Methodology Used:

For botnet detection author used Timestamp and frequent pattern set generation by the Apriori algorithm.

2.3 HTTP-sCAN: Detecting HTTP-Flooding Attack by Modeling Multi-Features of Web Browsing Behavior from Noisy Web-Logs

This paper author proposed anomaly-based HTTP-flooding detection approach abbreviated as HTTP-sCAN which is based on the density-based cluster algorithm.

HTTP-sCAN analyze the normal web surfing behavioral pattern by clustering multi-features of normal web users

in the presence of web-crawling traces, and then classify the attackers by comparing the individual web surfing behavior against the normal surfing. Also author considered the variation of popularity of webpage's, for that they designed a EW-MA-based scheme to update the webpage popularity dynamically.

2.3.1Methodology Used:

In this paper density-based cluster algorithm is used to analyze web surfing behavioral pattern and then compare it with individual web surfing behavior against the normal surfing to detect attackers.

2.4 A Netwo rk Behavior-Based Botnet Detection M echanism Using PSO and K-means

In this paper author proposed a mechanism that provides a simple and straightforward method to locate the Bot client. Proposed mechanism uses the three main network behaviors of bot client, Act Behavior, Fail Behavior, and Scan Behavior PSO+K-means clustering algorithm is used to predict the potential members of Botnet.

Mechanism uses the traffic flows, rather than the decapsulated packet contents, to locate the suspicious Bot clients.

The main advantage of this system is that user does not require to install various detection applications so it is suitable for dormitory network, a home network, and a mobile 3G network.

2.4.1Methodology Used:

In this paper PSO+K-means clustering algorithm is used to predict the potential members of Botnet

2.5 Botnet detection based on traffic behavior analysis and flow intervals

In this paper, author proposed that analyses traffic behavior and classify network traffic behavior using machine learning. Here traffic behavior analysis does not dependent on the packets payload, so that they can work with encrypted network communication protocols.

Proposed model allows detecting bot activity in both command and control and attack phases which is purely based on the observation of its network flow characteristics for specific time intervals.

2.5.1Methodology Used:

Author firstly studies various botnet detection machine learning techniques through network behavior analysis like Bayesian Network, Support Vector Machine and used decision tree classifier machine learning algorithm.

3. CONCLUSIONS

This survey paper explains about various detection techniques of HTTP Botnet detection. Because of the harmful effects of botnets and the considerable interest among the research community in this field, we proposed survey of botnet research which describe the botnet problem in global terms and provide different detection techniques. All detection techniques are based on the botnet's own life-cycle. This presents an interesting property every stage of the life-cycle must be effectively finished if the botnet is to succeed. Therefore, interrupting the execution of just one stage in the botnet life-cycle renders the whole botnet useless. For detection of HTTP botnet we can use signature based detection technique as well as behavior based detection techniques We have reviewed current research work in this field, and show that all defense efforts are in fact focused on one or more of these stages. This review is presented here as a survey of the most relevant contributions in the field.

REFERENCES

[1] G. Kirubavathi Venkatesh and R. Anitha Nadarajan, "HTTP Botnet Detection Using Adaptive Learning Rate Multilayer Feed-Forward Neural Network", Spinger,2012

[2] S.S.Garasia,D.P.Rana,R.G.Mehta, "Http Botnet Detection Using Frequent Patternset Mining "IJESAT,May-Jun 2012.

[3] WANg Jin1, ZhANg Min1, YANg Xiaolong1, LoNg Keping1, Xu Jie, "HTTP-sCAN: Detecting HTTP-Flooding Attack by Modeling Multi-Features of Web Browsing Behavior from Noisy Web-Logs", IEEE 2015.

[4] SHING-HAN LI , YU-CHENG KAO, ZONG-CYUAN ZHANG, and YING-PING CHUANG ,DAVID C. YEN "A Netwo rk Behavior-Based Botnet Detection M echanism Using PSO and K-means", , ACM Transactions on Management Information Systems , Volume 6 Issue 1, April 2015.

[5] David Zhao a, Issa Traore a , Bassam Sayed a, Wei Lu b, Sherif Saad a,Ali Ghorbani c, Dan Garant ba,"Botnet detection based on traffic behavior analysis and flow intervals" ACM Journal Computers and Security, Volume 39, November, 2013.

[6] Lai, G.H., Chen, C.M., Tzeng, R.Y., Laih, C.S., Faloutsos, C, "Botnet Detection by AbnormalIRC Traffic Analysis." JWIS 2009.

[7] Jae-Seo Lee, Tung-Ming Koo, Hung-Chang Chang,"P2P firewall HTTP-Botnet defense mechanis" , IEEE, PP. 33-39, 2011.