A Survey on Host Based Botnet Detection System

Adwait A. Rajmane[1,] Shreya B. Ahire [2]
1.Department of Computer Engineering, NBNSSOE, Ambegaon, Pune, Maharashtra, India
2. Department of Computer Engineering, NBNSSOE, Ambegaon, Pune, Maharashtra, India

Abstract

Botnets have today turned into one of the considerable threats to security systems. Botnets are believed to gain popularity among cyber criminals for attacking internet-connected devices from DVR players to corporate mainframes. Fake news on social media is spreading for social media bots and automated accounts. Cryptocurrencies like Bitcoin are also on the radar of cyber criminals who are mined using botnets. Botnets are very difficult to detect. Devices that are directly connected to the Internet or can be attacked or infected wirelessly. DDoS) can launch complex spam campaigns, launch massive financial fraud campaigns, and shake public beliefs with social media bots. In addition, as botnets continue to expand, many unusual things show a higher level of sophistication and anonymity, and it is more important to oppose them dramatically. Today, network security requires detecting various botnet threats and eventually ending them this section shows you how to implement a host-based intrusion detection system to detect botnet attack threats. This method is based on variations of genetic algorithms for detecting anomalies in the case of an attack.

Keywords*: botnets, genetic algorithms, intrusion detection systems, bots, intrusions, security, threats, hosts, IDS, distributed denial of service DDoS, spam, malware, MAC address.*

I Introduction

Botnets are considered to be one of the most serious outbreaks of modern malware. One of the fastest evolving problems today is botnets that are well understood and unresearched. A botnet is a collection of infected computers running malware, meaning a group of bots and controlled by hackers. We have a centralized infrastructure for control. A centralized infrastructure is called a C&C centre. C&C structure is likely to have a malicious type and may illegally control bot computing resources. Botnets are believed to gain popularity among cyber criminals for attacking internet-connected devices from DVR players to corporate mainframes. Fake news on social media is spreading for social media bots and automated accounts. Cryptocurrencies like Bitcoin are also on the radar of cyber criminals who are mined using botnets. Botnets are very difficult to detect. They can attack or infect almost any device that is directly connected to the Internet or wirelessly. DDoS can start, tackle complex spam campaigns, launch mass financial fraud campaigns, and shake public beliefs with social media bots.

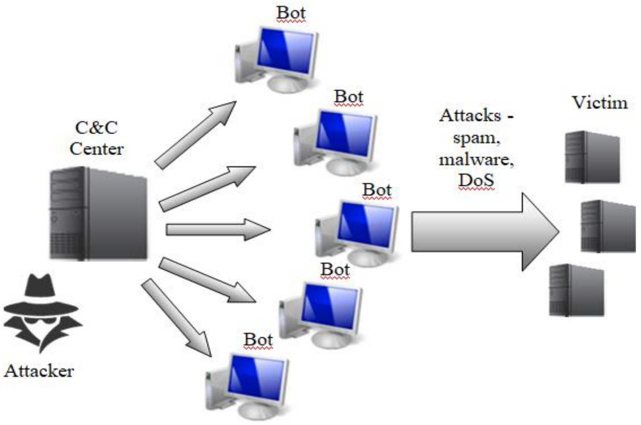


Fig. 1 Botnet Structure

One of the core uses of botnets is to achieve denial of service (DoS) attacks. This type of attack is performed by releasing a large number of packets from one or more sources at the same time. The main purpose is to surplus the destination device otherwise creates or perform congestion of the transmission channel towards attacked system. Most network attacks around the world are considered botnets. One of the biggest reasons for network attacks around the world remains the trend of botnets. One of the key areas of network security in modern times is to create satisfactory or acceptable technologies for botnet detection and final botnet removal[11]. Existing botnet detection systems use systems that primarily detect anomalies and based on rules. One of the significant tasks is to create a profile of the regular behaviour of the system. Once normal behaviour is recognized, the system can be used to detect anomalies based on the profile sit-up.

This survey paper introduces the intrusion detection system (IDS) approach used to detect botnet attacks on a host basis.

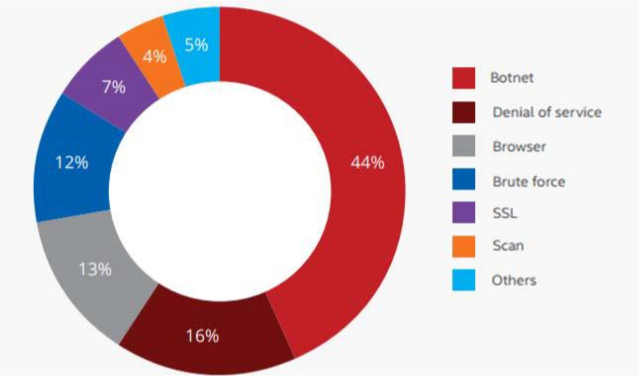


Fig. 2 Global network attack

II Motivation

Malware is considered a significant cause of cyber-attacks that are rapidly increasing in the form of botnets. A botnet is a group in which the compromised machine is remotely controlled by a central server, and a compromised machine called "bot" is connected to a central server that operates by "bot master", which gives the order of execution. According to a survey, botnets are emerging rapidly as a threat to infect ten million of computers, around 40% of wholly computers connected to the Internet around the world are infected by infected bots and controlled through hackers. Botnet research can be classified hooked on three areas: understanding botnets, detecting and tracking botnets, and defending against botnets. Botnet malware does not target specific individuals, rather look for vulnerable devices on the Internet in companies and industries. Many connected devices are possible to use resources for automated tasks that can be economically and socially damage while hiding in users and devices[12]. Therefore, due to the increasing and disastrous effects of botnet attacks, it is necessary to create an approach for intrusion detection or botnet detection to prevent economic and social harm.

III Literature Survey

Sr. no	Year	Author	Paper	Methods	Advantages	Disadvantages

1	2019	Yulia Aleksieva, Hristo Valchanov	An Approach for Host Based Botnet Detection System	Host Based	Intrusion Detection and Identification	Even if we detect botnets it will not stop cyber-attacks.
2	2019	Thomas Lange, Houssain Kettani.	On Security Threats of Botnets to Cyber Systems	Research study	Understanding botnet and it's threat to cyber systems.	Botnets are a threat to cyber security.
3	2019	Oleg Savenko, Anatoliy Sachenko	Botnet Detection Approach for the Distributed Systems	Approach for the Distributed Systems	Botnet Detection and Identification	Accuracy of botnet detection is 88%
4	2019	Shogo Maeda, Atsushi Kanai	A Botnet Detection Method on SDN using Deep Learning	Deep learning	Infected machines are isolated after detection using a deep MLP model Learning.	Need to explore and you can isolate the network in the case of actual infection. Host.
5	2018	Rohan Bapat, Abhijith Mandya	Identifying Malicious Botnet Traffic using Logistic Regression	Logistic Regression, Machine Learning	Botnet Detection and Identification	More supervised learning methods need to be applied.
6	2018	Kamal Alieyan, Rosni Abdullah	A Rule based approach to detect Botnets based on DNS	DNS	Botnet Detection and Identification	Accuracy is less
7	2018	Shao-Chien Chen, Yi-Ruei Chen	Effective Botnet Detection Through Neural Networks on Convolutional Features	Convolutional neural networks	Botnet Detection High Accuracy	None
8	2017	Basil Alothman Prapa Rattadilok	Towards using Transfer Learning for Botnet Detection	Transfer-Learning	Botnet Detection and Identification	Traditional machine learning not used

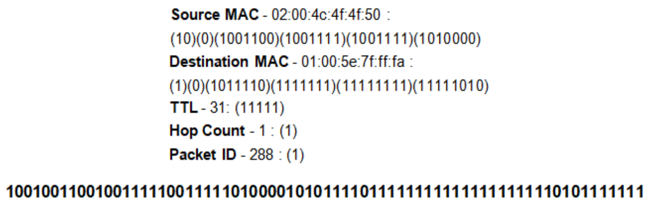
9	2017	Manoj S. Koli Manik K. Chavan	An advanced method for detection of botnet traffic using Intrusion Detection System	Machine learning	Botnet Detection and Identification High detection accuracy (99.984%)	Cannot deal with small scale networks
10	2017	Yuan-Chin Lee Chuan-Mu Tseng	A HTTP Botnet Detection System Based on Ranking Mechanism	Machine learning	HTTP Botnet Detection	Behaviour ranking mechanism is variable
11	2017	Bhan Sengar Professor.B.P admavathi	P2P bot detection system based on Map Reduce	P2P	Botnet Detection High Accuracy	Data size reduces then processing time increases
12	2017	Gernot Vormayr, Tanja Zseby	Botnet Communication Patterns	Communication Patterns	Understanding Botnet Communication Patterns	None

Table 1 Literature Survey

IV SYSTEM ARCHITECTURE

A. Packets and chromosomes

The following method for parsing processed packets, uses specific variations of genetic algorithms. The difference is based on the choice of genetic active and evaluates all individuals of a successful generation and it is based on an analytically determined fitness function. For every single organism, they have their personal individual plans encoded in their genes. Chromosomes are formed by connecting these genes, and these chromosomes form organisms known as phenotypes. In this case, we treat the received packets as phenotypes. After chromosome formation, they are analysed, and the change is detected by phenotype and mutation.



Source MAC - 02:00:4c:4f:4f:50 :
(10)(0)(1001100)(1001111)(1001111)(1010000)
Destination MAC - 01:00:5e:7f:ff:fa :
(1)(0)(1011110)(1111111)(11111111)(11111010)
TTL - 31: (11111)
Hop Count - 1 : (1)
Packet ID - 288 : (1)

100100110010011111001111101000010101111011111111111111111111110101111111

Fig. 4 Forming a chromosome from a packet

In this papers algorithm, genes are extracted from the resulting packet (phenotype), which are bound to the verification chromosome. The attributes of the packet used as a gene are as follows:

- Source Mac address;
- Destination MAC address;

- Source IP;
- Protocol number
- First time to live;
- Hop count;
- Packet ID.

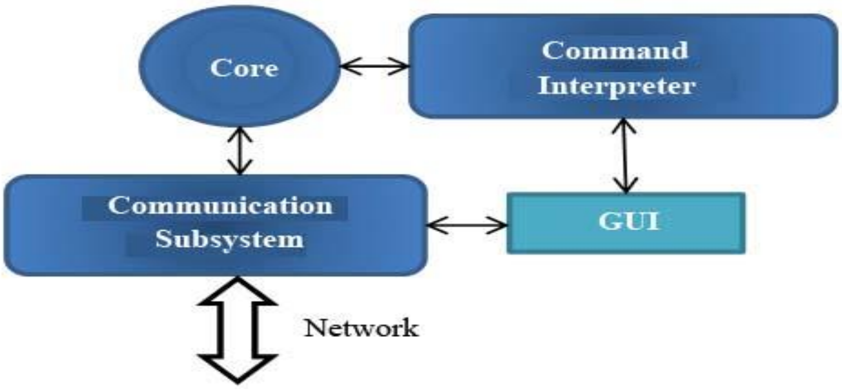


Fig. 3 Intrusion Detection System Architecture

If an attacker attempts to perform a spoofing attack, all of these genes can be changed because they are variable. Packet chromosomes are obtained by converting the values of these genes into binaries and linking them using algorithms. The validity of a packet identifier is represented by last bit of the chromosome, but it does not represent the identifier itself. If the packet ID is greater than the previous packet sent from the similar source, packet ID is supposed to be '0'. If a valid packet sent consistently from the identical source does not have a healthy incremental identifier, here is an assumption that external interference is occurring while transferring packets that could attempt to attack.

B. Fitness features

An analytical calculation among two chromosomes, that is, two packets received from the same source address is a fitness function. The mathematical fit of the received packet is calculated and the two chromosomes are compared bitwise. When a packet is first received from an IP address to the system, the chromosome is formed from that gene and stored at a fitness level of 100%. Subsequent verification is carried out using the chromosome as a pattern. The fitness level of each packet is also calculated by applying the fitness function. The minimum fitness level of the acceptable system set as chromosomal fitness of 65%. After observation and analysis on the system in a normal and attack environment, we selected above number. Selecting this number lowers the result of the false positive.

If you get a satisfactory level of about 65%, after comparing chromosomes on average, it means that there is low level matching, and therefore the system generates an attack alarm.

Packet attribute	**Max length (bits)**
Destination MAC	48

Source IP Address	32
Source MAC Address	48
Hop Count	8
TTL	8
Packet ID Validity	1
Total	145

. Table 2 Chromosome Length

V Conclusion

Various tools, such as intrusion detection systems, help you achieve your goal of countering and mitigating threats. The above system presented an approach to creating and implementing a host-based system to detect botnet attacks. Anomaly detection technology is used by systems based on variations of genetic algorithms that analyse traffic passing through the host's network interface. Each packet received is analysed individually by the algorithm to determine whether a spoofing attack caused external interference.

VI FUTURE SCOPE

In the future, you can extend the capabilities of your system by providing several techniques for detecting anomalies, includes adding data integrity analysis. You can also integrate technology, a signature-based technology that can detect already known attacks quickly, quickly and systematically.

References

[1] Yulia Aleksieva, Hristo Valchanov et al., “An Approach for Host based Botnet Detection System” XVI-th International Conference on Electrical Machines, Drives and Power Systems ELMA,Varna, Bulgaria,2019

[2] Thomas Lange, Houssain Kettani, “On Security Threats of Botnets to Cyber Systems” 6th International Conference on Signal Processing and Integrated Networks (SPIN),2019

[3] Oleg Savenko, Anatoliy Sachenko et al., “Botnet Detection Approach for the Distributed Systems”The 10 th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications,Metz, France,2019

[4] Shogo Maeda, Atsushi Kanai et al., “A Botnet Detection Method on SDN using Deep Learning”2019

[5] Kamal Alieyan,Ammar Almomani et al., “A Rule Based approach to Detect Botnets based on DNS” 8th IEEE International Conference on Control System,Computing and Engineering(ICCSCE 2018),Penang,Malaysia,2018

[6] Rohan Bapat, Abhijith Mandya et al., “Identifying Malicious Botnet Traffic using LogisticRegression”2018

[7] Shao-Chien Chen, Yi-Ruei Chen et al., “Effective Botnet Detection Through Neural Networks on Convolutional Features”,17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering,2018

[8] Basil Alothman and Prapa Rattadilok, “Towards using Transfer Learning for Botnet Detection”The 12th International Conference for Internet Technology and Secured Transactions (ICITST-2017)

[9] Manoj S. Koli and Manik K. Chavan, “An advanced method for detection of botnet traffic using Intrusion Detection System”International Conference on Inventive Communication and Computational Technologies (ICICCT 2017)

[10] Yuan-Chin Lee Chuan-Mu Tseng et al., “A HTTP Botnet Detection System Based on Ranking Mechanism”The Twelfth International Conference on Digital Information Management,Kyushu University, Fukuoka, Japan.2017.

[11] Dr. C. Nalini, Shwetambari Kharabe, Sangeetha S,” Efficient Notes Generation through Information Extraction”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6S2, August 2019.

[12] Shwetambari Kharabe, C. Nalini , R. Velvizhi,” Application for 3D Interface using Augmented Reality”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-6S2,August 2019.