e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

AN ADVANCED METHOD FOR DETECTION OF BOTNET USING INTRUSION DETECTION SYSTEM

Alan Saji[*1], Milan Sha[*2], Raichan Kuriachan[*3], Denny P Francis[*4]

[*1,2,3]MG University, Department Of Computer Science, De Paul Institute Of Science & Technology, Angamaly, Kerala, India.

[*4]Asst. Professor, Department Of Computer Science, De Paul Institute Of Science & Technology, Angamaly, Kerala, India.

ABSTRACT

A botnet, especially with remote-controlled bots that provides a platform for many cyber threats. The effective measure against that botnet is provided by IDS (Intrusion access system). The IDS regularly monitors and identifies the presence of effective attacks by assessing network traffic risks. The IDS (PI-IDS) check for payload detects active attempts to test the user's data gram protocol (UDP) and transmission control protocol (TCP) comparisons with known attacks but the PI-IDS process is destroyed if the package is encrypted. PI-IDS shortages are overcome by Traffic-based IDS (T-IDS), do not check package load; instead, it checks the packet header to separate access, but this process is not suitable in today's world because network traffic is growing rapidly so looking at the header of each packet is not working properly and because of this gain rate is also important. Therefore, we put forward an approach to this paper T-IDS creates an RDPLM (data-readable learning model) based on the set features, as well as a feature selection process, simplified sub spacing and multiple randomized meta-learning techniques .The accuracy of our model is 99.984% and the training time is 21.38 s on a well-known botnet database. It has been found that some mechanical learning models resemble a deep neural network, reducing errors in pruning the task of finding a drug in a very small sequence, and a random tree. Keywords: Telecommunication Traffic, Feature Extraction, Protocol, Intrusion Detection, payload, computational modelling.

Keywords: Telecommunication Traffic, Feature Extraction, Protocols, Intrusion Detection, Payloads, Computational Modeling.

I. INTRODUCTION

Today, our reliance on the Internet has grown exponentially. As well as the need to protect our comprehensive information available through the web interface such as Internet passwords, company secrets, online bank accounts, and social networking accounts such as Facebook. The emergence of bottles in the online space over the past decade, and their ever-changing behaviour has created real challenges that cannot be easily remedied. According to documents, botnet is set as a group of infected administrators (also called bots or zombies) that operate independently and automatically, controlled by a botmaster (bot shepherd) who can combine his malicious intent using infected bots. Some of the vulnerable activities that can be infiltrated by botnets include DDoS (Distributed denial-of-service), spam, sensitive identity theft, ransomware and data theft. In a DDoS botnet attack, a botmaster may order all its bots to attack a particular server (for example: update.microsoft.com) on a specific day, time and time with a malicious or anonymous proxy used as a hideout for the actual command node. In a spam campaign, the nodes that make up the bot network are responsible for sending spam behaviorally as spam forwarding points, bringing spam emails to a list of targeted email addresses selected by the bot master. For instance : a node that is part of a dangerous botnet can be sent a list of email addresses to spam of the day by the spam upload to be mailed. These spam messages can advertise pharmaceutical products and may also cause more infections As noted in many papers (Provos et s via email links or attachments to get more bots, as is done with bottles like Storm and Waledac . It is a scam to steal sensitive information that works to act as we proxies or web servers to send hoax content to malicious users in order to collect their E-banking or credit card details. For example, sites may hold content that looks like a banking site requesting login information when a user submits it, may be used by a plant company to find legitimate banking sites. Eventually funds are transferred to non-stop accounts (Nazario & Holz 2008). Storm-like botnets are known to have infected more than 2 million while Conficker has infected more than 9 million

on the basis of some estimates. As can be seen the, far-reaching effects of the vicious intent of the bottles and their masters are a real danger.

II. LITERATURE REVIEW

One of the hottest research topics is botnet detection. Much research in the literature focuses on botnet detection techniques. Many of these methods focus only on a specific type of botnet. Botnet behaviour based acquisition methods can be divided into three categories: host-based detection, network-based detection, and hybrid detection. Here, we briefly describe some previous research that suggests various botnet detection solutions.

2.1. Botnet-Detection at the Host Side:

Using antivirus software and firewall to protect the homeowner is not enough to prevent its infection with botnet malware. In addition, even if we can stop the C&C server, the infected host (via bot) can be restarted in future attacks. In this case, we need a host-based acquisition to complete the bot program on the host. There are various studies on host-based techniques [9 - 11]. Huang [10] proposes a practical solution for finding a bot host based on tracking network failures in the short term. The solution consists of two phases: (1) the training phase and (2) the acquisition phase. The first stage is used to remove the elements from the flow of failure. The second phase analyses data based on the facts obtained during training using the C4.5 algorithm. In [9], Etemad and Vahdani undertook the discovery of a C&C-based botnet through a host analysis. Their solution is based on the analysis of real incoming and outgoing traffic. It has two basic features: (I) Protocol Coordinator: outbound traffic and inbound traffic is redirected to this section. First, this section of the protocol separates IRC traffic and HTTP protocol from the entire host. After that, it transmits the separated traffic to the interpretive part of the communication pattern. (I) Communication pattern translator has two modules: IRC module and HTTP module. This section separates malicious traffic from official traffic. After that, the host firewall can filter this malicious package. In the IRC module, it detects a malicious IRC bot based on its communication traffic and botnet C&C server. In the HTTP module, it detects botnet C&C server communication based on the HTTP message timeline pattern.

This method is based on the traffic analyst on the host and not on finding the process. It does not process encrypted packets (command) from the botnet master to bots. In addition, it is limited to one botnet and does not work with P2P botnet.

In [12], Zeng et al. proposed content level for each process level for each manager in the target network. The content of each process consists of two elements: the behavioural analysis component and the content model. The behavioural analysis section contains various monitoring generators and process suspicions. Process is based on operating time behaviour at the operating system register, file system, and bulk network. After that based on the study of the process functions, they used the SVM algorithm for each active process to give a suspicious level of that process. In the containment, there is an optimization method optimizer to pass suspicious points to the threshold of each process.

The way they work has many high-level:(1) They propose a process that combines both ethical analysis and early security protection and automatic protection in opposing to dangerous network threats.(2) They create a dubious level for each process using a machine learning classification process and make an algorithm for drawing each suspicious mark of the standard at the limit of the measurement process. (3) They do a careful and deep observation and searching using real-world insect trails and general systems.

2.2 Network Based Bot-net Detection:

Previously, botnet detection strategies were based on payload analysis methods that test the content of TCP and UDP packets for malware signature. Payload analysis techniques consume resources that need processing huge amounts of package information and are a slow process. In addition, the new generation of botnet uses encryption algorithms and other methods to encrypt communication traffic and crush load loading analytics techniques.

Flow-based signals released from network tracking were alike to Net-Flow features like bytes per packet, byte-per-flow, and bytes per second. Over the past few years, strategies have been developed to find a botnet using streaming content. There are many ways to get the proposed network traffic over the years in this part, a arguement of some of these strategies and their restriction will be discussed. Anomaly discovery can be a

mining-based acquisition technique used to extract unexpected network patterns. Therefore, it can get unusual traffic even if packets are encrypted. Numerous strategies have used flow analysis [5, 7, 13-15]. In [5].

Standard botnet detection capable of finding several types of botnet is proposed. This method analyses network traffic during fixed periods. After that, the integration of the data into the flow of the network is designed to create an effective division system. This method can detect the botnet either the topology or the protocol used. In addition, it can detect anonymous botnet. In [7], Liao-and-chang proposed a way to find a P2P botnet based on analysing and monitoring network traffic using a data mining system. They tested their solution using 3 popular data mining targets: J48, naïve Bayes, and Bayesian-networks. The accuracy of the algorithms is 97% 87%, and 89%, respectively.

Zhao-et al. in [13] put forward a new P2P solution for botnets by analysing network traffic. Their idea consists of choosing twelve attribute from the network flow to be analysed and therefore excluding the flow of the pre-defined time window. They use machine-learning algorithm separate botnet traffic from official traffic. They select the decision-tree the reduced error algorithm error. After that, they use the integration signer checker to select the cold key attribute for bot-net detection. Their method can detect the activity of a single bot offline or in live traffic. In addition, it is able to find secret bots and find bots in the first phase through its work in the C&C section.

Hung. and Sun. in [14] put forward a bot-net detection mechanism based on machine learning. The solution depends on network traffic. Initially, a group of flow-based features is selected and extracted from network traffic. After that, to ensure the model is working properly, some sound is added to the payload, duration, and features. This solution achieves a high accuracy of up to 99.7% on some botnet types. Compared to the live bot-net detection system, the put forwarded solution represents that it can withstand a lot of noise.

Alunthaman-et-al. [15], a P2P bot-net suggested acquisition program on the basis of the decision-tree and multilayer neural networks. This framework only monitors network traffic to detect bot-net communication with the C&C server and between bots. First, network mitigation is done to manage the maximum amount of network traffic. Subsequently, 29 aspects of bot-net detection are proposed. Factors that have a small influence on the split model are removed using a feature reduction method: tree separation and reversal (CAR). The goal of this reduction is to keep only the relevant features to obtain the best values for neural-network learning and phase accuracy. Testing of this method shows that it provides excellent accuracy by 99.2% and exceeds the available solutions.

DNS detection strategies are based on analysis of specific DNS features generated by bot-net. However, these Domain Name Server methods do not help to differentiate C&C server. Traffic from new botnet models. Some solutions center on Domain Name Server traffic to find a botnet that transfers to DNS to find a C&C server.

Zhao-et-al-[16] we suggest the ID ns system detects malicious domain names on the C&C server for A.P.T attacks (the main threat). The proposed system has been used on the network side which can lessen the amount of network traffic to be registered and analysed. Their approach contains of 4 elements: (I) Data Collector: to keep incoming and outgoing network traffic. (I I) Bad DNS identifier: to update a DNS record kept by a data collector. After that, if finds the malicious APT and C&C Domain and provides the suspicious IP-related Internet Protocol address in the following items. (I ii) Part of the road analyst: has two units that are a signature detector and an unidentified detector. (Iv) Fame Engine: calculates the reputation results for every Interne t Protocol address from previous episodes. The 14 elements studied by a sucpicious Domain Name Server finder in this method are categorised into five types: domain name features, DNS response features, time-value features, TTL-based features, and active test features. This botnet detection can only detect DNS-based malwares. Therefore, the P2P botnet is not available.

2.3 Hybrid-Based-Detection:

acquisition is the link between network analysis and traffic analysis. Zeng-et-al[17] suggested a bot-net detection process that includes noth host detection and network detection. Their solution is first and foremost, which includes network-level detection and linking alerts that can increase access accuracy. They recommend using 9 features of host analysis: Six features of file and subscription and 3 features of network traffic on the host. Network analysis, 17 features are extracted from net f low data. They tested the integrated network hosting process and showed that their solution worked compared to I.R.C, P2P and Hyper Text Transfer

Protocol bottles. In [17], a bot-net detection process that accomodates both host level detection and network-level detection is developed. The suggested solution, called E.F.F.O.R.T is designed as a way to link data from various aspects of hosting and network level to achieve effective and efficient detection. The solution is made and tested with real word machines. The outcome shows that E.F.F.O.R.T successfully detects up to 15 real-word bots with a low level of lies. In 19 Abdullah-et-al manage P2P board construction. Their solution hangs on the interaction between the host and the network. At the hosting level, the study will be in the file system: register and log file. This analysis looks at abnormal behaviours and characteristics in each and every single activity that has occurred in the host. At network level, the study is a complete package upload. This analysis can separate both C&C servers and infected administrators by bots in the network This solution can also be considered a form of protection. In fact, it works well for finding a bot in the first phase from host analysis. Any howk, it takes time to finish the analysis because of network violations on P2P bots. In terms of correct detection rate, it merges the result the result of host analysis with the result of network analysis.

III. DISCUSSION

We have introduced a small state of the art in relation to botnet-detection, which contributes significantly to the local and regional access to bots. We found the difference between (1) botnet-detection on the host site, (2) botnet-detection on the network site, and (3) hybrid botnet-detection. It is pellucid that the largest benefits will be achieved through a solution that (I) Combines hosting and network analysis that means the acquisition of a hybrid botnet: for efficiency, some solutions include many strategy. Used to detect hybrid botnet, many parameters are integrated and integrated to create a local and acquire an unusual character. 1In this situation, if bot traffic is not identified by the network analyser, the host analyzer can identify it using other protocols and consider other factors and the opposite is correct (if the bot's behaviour is not identified by the host analyst, the network analyser may find it using other protocols and consider others features). (ii) Reducing the difficulty: the purpose of the botnet-detector is to identify botnet traffic early while reducing the difficulty and processing time of the analyst. For example, a network analyser should analyse and separate all incoming and outgoing traffic. As a result, an efficient botnet detector must filter traffic before starting analysis. (I ii) Easily adjusted to detect new and intrusive botnets: a botnet detector can have a good rate of detecting 1known botnets. However, the solution should also identify an unknown botnet with very high accuracy. In all situations, the purpose of all these solutions is to identify the botnet immediately and to stop it. The best solution is to get a 100% adoption rate with a 0% false positive rating. In order to be accepted, such solutions must work with minimal difficulty and be able to obtain new or unknown bottles.

IV. CONCLUSION

In this study, we proposed a standard procedure that can detect a new botnet used 1on 3 levels: the level of hosting, the level of the network, or a combining both. Our favourite botnet communication traffic 5contains HTTP, P2P, IRC, and DNS using IP fluxing. Our proposed process 1contains of 3 components: a host analyzer, a network analyzer, and a discovery report: (i) A network analyzer looks at two functions: botnet distribution and botnet communication with a C&C server. The network analyst contains three detectors: distributor, P2P detector, and non-P2P detector. (I i) The host analyst evaluates three functions: registration keys, file system, and the process time over time. The host analyzer has three components: behavioural analysis, process integration, and process ethics. (I ii) The acquisition 1report is responsible for making the final score of the points based on the analyst's analysis or network analysis and provides for the report of the infected equipment. We have developed the HANA Bot algorithm to process hosting traffic data, the performance of hosting processes, and the function of the road 2network to identify bots according to certain rules. All botnet flow records are successfully extracted using specific 1connection process and setting object vectors that differ from the botnet network traffic and the performance of its process. A comparison between the existing method was provided, focusing on specific features and performance. In our future work, we will apply our solution to real-time separation. In fact, the suggested process uses an offline mode separation algorithm, in which the Internet network tracking is stored in a P.C.A.P file prior to processing them. This method can be developed to detect real-time detection quickly with a high degree of precision. This can be attained by creating the Net flow collector's export time much shorter and by providing Net flow clues sent to instant separation technology, as they arrive. This method can detect botnet activity and, on this basis, the action to be taken. The speed of processing done in real-time phases should be different, depending on a variety of factors, such as the duration

of posting and size of the Net flow tracked channels. In addition, this function can be extended, at the hosting level, to bear the needle detection process used by the botnet to fully control the process [35].

V. REFERENCES

[1] M. Sanchez, "The 10 most common security threats explained," 2017.
[2] http://blogs.cisco.com/smallbusiness/the-10-most-common-security-threats-explained.
[3] Us.norton.com. (n.d.), "Bots 2017, https://us.norton.com/botnet/.
[4] B. Cusack and S. Almutairi, "Listening to botnet communication channels to protect information systems," in Proceedings of the Australian Digital Forensics Conference, pp. 44–52, Joondalup, Australia, December 2014.
[5] DDoS attacks in Q1, 2018, https://securelist.com/ddos-report-in-q1-2018/85373/.
[6] Kirubavathi and R. Anitha, "Botnet detection via mining of traffic flow characteristics," Computers & Electrical Engineering, vol. 50, pp. 91–101, 2016.
[7] J. He, Y. Yang, X. Wang, Y. Zeng, and C. Tang, "PeerSorter: classifying generic P2P traffic in real-time," in Proceedings of the 2014 IEEE 17th International Conference on Computational Science and Engineering, pp. 605–613, Chengdu, China, December 2014.
[8] W. H. Liao and C. C. Chang, "Peer to peer botnet detection using data mining scheme," in Proceedings of the International Conference on Internet Technology and Applications, pp. 1–4, Wuhan, China, August 2010.