International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

A REVIEW ON BOTNET DETECTION AND MIIGATION IN ADHOC NETWORKS

Mariya Ameer[1], Manish Kansal[2]

[1]Research Scholar,Dept of Electronics and communication, PEC Mouli, Kurukshetra University,Haryana,India
[2] HOD, Dept of Electronics and communication, PEC Mouli, Kurukshetra University,Haryana,India

---

ABSTRACT-*Botnets are the networks of remotely controlled computer systems infected with a malicious program that allow cybercrimes to control the infected computers or machines without the user's knowledge. Botnets are the most ever-growing much interested evolved in the design of mobile adhoc networks (MANET).A botnet in mobile network is defined as a collection of nodes containing a malware called mobile malware which are able to bring the different elements into harmonious activities. Unlike Internet botnets, mobile botnets do not need to propagate using centralized structure. With the advent of internet and ecommerce application data security is the most critical issue in transferring the information throughout the internet. Botnets are emerging as the most significant threat facing computing assets and online ecosystems. The sharing of information through internet has been the main driver behind the Elite hacker into criminal activities. Their main target is to steal the vulnerable information from the individuals or from the organizations .In other words we can say their purpose include the distribution of spam emails, coordination of distributed denial of service (DDoS) and automatic identity theft. This paper provides an extensive analysis of all the work related to this field that has been done in the recent past.*

KEYWORDS: Botnet, Bot, Botmaster, Rootkit, MANET, Zombie. Mitigation and detection.

1.INTRODUCTION *(Size 11 , cambria font)* A modern definition for the bot can be defined by the worms, viruses, Trojan horses and rootkits that incorporates usually one or more techniques introduced by the worms, viruses, Trojan horses and rootkits for propagation into a foreign system. A main defining characteristic is that after forming botnet system they can connect back to the central serve or any other infected machine after compromising. Botnets in today scenario are the biggest challenge for the security researchers and analysts. The most important part of the botnet is its command and control(C&C) architecture. The Botnet architecture consists of a control entity that can be either centralized or distributed together with a bot. Here to command the victim computers and to manage their actions protocols are used by the botmaster. The downloading of the software program is the initial stage of botnet. These malicious software will then compromise the machine and use it for the criminal purposes. A typical botnet can be created in five phases including initial infection, secondary. Injection, connection, malicious command and control, update and maintenance. In the initial infection, the attacker infects the victim machine through various methods and scans the target subnet for known vulnerability. After this phase there comes the injection Stage where an infected host executes a shell code which fetches the image of the actual bot binary via a specified location such as http and ftp. This bot install itself on the target machine called zombie which runs the malicious code. In connection phase the program called bot program establish a command and control channel and connects this zombie machine with command and control server. Here the zombie becomes part of attacker's army. Here the command and control channel enables the botmaster to control the action of large number of bots. Last phase include the maintenance of lively bots. Today, a primarily motivation for operating a Botnet is the income that can be earned from sending spam emails. Another popular source of income for online hackers is the installation of advertising software, known as adware. Most of the adware software companies provide monetary incentives. Today phising schemes are also a major revenue generator.

In view of the increasing demand for the wireless information and data services, providing faster and reliable mode access is becoming an important concern. A Mobile ad hoc network (MANET) is a network called spontaneous network that can be established without any infrastructure or any kind of topology. It means that all nodes behave as a router and participate in its discovery and maintenance of the routes. Its routing protocol has to be able to manage new difficulties that an ad hoc network creates such as node mobility, limited power, quality of service, and

bandwidth issues. The challenges defined above create set new requirements on MANET network with routing protocols and make them more exposed to attacks. In MANETS, all the participating nodes are involved in the routing process. Since conventional routing protocols are designed for predefined infrastructure networks, which cannot be used in mobile ad hoc networks so new routing protocols were designed to accomplish the requirement of less infrastructure ad hoc network

1.1 Literature Review

Among the various forms of malware attacks, botnets are the major serious threat as they provide a distributed platform for several illegal activities. A defining characteristic for the botnet is the command and control channels through which they can be updated and directed. For the botnet detection several techniques can be implemented [1]. Moreover, the botmaster doesnot physically own the bots as they may be located in several positions spanning the globe. Differences in time zones, languages, and laws make it difficult to track malicious botnet activities across international boundaries A method for the Mobile ad hoc network for the security against botnet involves the use of hybrid CS by making use of clustering method. Here the mobile nodes are organized into clusters and botnet detection can be made by making use of both anomaly and signature based IDS [2] using watchdog timer. The nodes called the mobile nodes that are organized into clusters, transmit the data to cluster head (CH).These cluster heads then transmit data to sink nodes. An analytical method can be used to find the relationship between the size of the clusters and number of transmissions in the hybrid CS. Because of the advance in the Internet technology, the applications of the Internet have become much chronic.

We see the number of mobile devices used globally substantially increasing daily, therefore information security concerns are increasingly vital. As Botnet being the major threat in today's scenario, for mobile devices we can use a feature selection method for detecting botnet viruses[3]. The botnet virus is a major threat to both mobile devices and personal computers. In LAN environment having many computers that has been infected by the virus called botnet virus that can be simulated for testing. We see in practical applications, classification accuracy is typically the first priority with detection speed being as crucial as accuracy. To obtain the desired detection speed the data required must be reduced for processing under the premise that the accuracy level is the same. Various methods can be used for identifying the critical features that define the pattern of botnet. A plan of action designed to achieve strategies for defense against botnets with measures and activities should be carried out for the successful defense [4]. It is necessary for IT community to develop effective techniques for detecting and mitigating the malicious behavior of the botnets.

Nowadays IT security involves a lot of field and variety of security aspects, starting from the lowest layers of OSI models up to applicative ones. Since the security of lowest layers of this model has been improved so the attackers are moving towards the higher layers of this model. In most of the cases they make their entrance via the application layer. Because of the fast growing internet that has been simulated by various services such as transferring and updating the information separately from the software platforms, question of security has become much more crucial.

Also network traffic monitoring and analysis-related research has struggled to scale for massive amount of data in real time. We see some of the vertical scaling solutions can be used for the botnet detection but unfortunately these approaches do not work if attacks originate from multiple machines at a lower speed, like the scenario of P2P botnets. However a scalable packet capture module to process in a quasi-real-time for high bandwidths of data can be used to provide distributed feature extraction framework to characterize flow statistics of packet capture and a peer to peer security threat detection module which classifies malicious traffic on cluster [5] Some recent botnets have used distributed C&C architecture (e.g. P2P), mainly to avoid single-point-of-failure problem. Also, nowadays newer P2P botnets are making use of advanced techniques like Rootkits, Fast flux. A proactive botnet detection framework using support vector machine(SVM) for the identification of P2P Botnets can also be used based on payload independent statistical features[5][6]. This investigation is based on the assumption that there exist a significant difference among flow feature values of P2P botnet traffic and that of normal web traffic. Here combination of the normal web traffic and normal P2P traffic can be used for the purpose of binary classification by evaluating the optimum SVM model that provides the best classification of peer to peer botnet data.

We see network security applications often require analyzing volumes of data to identify abnormal patterns or we can say activities .Today a novel system called Bot Graph [7] can be used to detect a new type of botnet spamming attacks targeting major web email providers. Bot Graph uncovers the correlations among the botnet activities by constructing large user-user graphs and then looking for tightly connected sub graph components. This enables to identify stealthy botnet users that are much harder to detect in isolation. To deal with the huge volume of data, we can implement Bot Graph as a distributed application on a computer cluster can obtain a variety of optimization techniques. It has been seen that for constructing and analyzing a 220GB Hotmail log requires running time of around 1.5 hours with 240 machines. By implementing graph based approach a wide class of security applications can be applicable for analyzing a large datasets.

Botnets are the prevailing mechanism for the felicitation of the distributed denial of service (DDoS) attacks on the computer networks [8]. Currently, we see Botnet-based DDoS attacks on the application layer are the latest and problematic trends in security threats. The botnet based DDoS attacks on the application layer limits resources, curtails revenue, and yields customer dissatisfaction, among others. DDoS attacks

are among the most difficult problems to resolve online,especially when their target is web servers. A distributed Dos (DDoS)attack is launched by a mechanism called botnet by making use of large number of controlled computers. A software program then controls the computers and for specified purposes, known as " bot". The goal of a Botnet based DDoS attack is to entail damage at the victim side. In other words we can say the ulterior motive of these attacks is to block the available resources or degrade the performance of the service. Another purpose aims to gain popularity in the hacker community. In addition to this, these attacks can perform for the material gain, which means to break the confidential data and use that data for their use. As a lot of sophisticated duties are being migrated to mobile phones, they are gradually becoming hot targets of hackers. Day today we see a lot of sophisticated duties are being migrated to mobile phones, thus are gradually becoming the hot targets of hackers. However we can design a bot using a short message service(SMS) as its command and control medium.[9].We see botnets are the current scourge of the internet that may result in the high rates of the TCP sync scanning or distributed DDoS attack[8].]By combing with a IRC parsing component with a sync scanner detection system aiming at individual IP host we can overcome the botnet problem. The IRC component produces two tuples, one is used for determining the IRC mesh based on IP channel names, and a sub-tuple which collects statistics on individual IRC hosts in channels. The number of scanners producing a sorted list of potential botnets sorts the channel. By deploying in PSU's DMZ helps in reducing the number of botnet clients. However by using a trivial cipher to encode the IRC commands it becomes more robustic for detection means.[10]

2. CONCLUSION

An extensive review of some of the important works relating to this field is done in this paper. The paper describes the main techniques utilized by each author along with a brief summary of their results and the limitations. It is found a lot of work is done in detecting and mitigating Botnet problem. Incidents around the world and revenue losses of famous companies and governments web sites are indicating that an extreme care should be taken and a further research should be conducted to assess the size of the problem and derive an optimal solutions.

REFERENCES

[1] Maryam Feily,Alireza Shahrestani and Sureswaran Ramadas"A Survey of Botnet and Botnet Detection ,National Advanced IPv6 Center of Excellence (NAv6)IMPACT Research Team University Saints Malaysia (USM)Penang, Malaysia, Faculty of Computer Science and Information Technology University of Malaya (UM), NAv6 2009 Third International Conference on Emerging Security Information, Systems and Technologies

[2]HemalathaU,Mohana.P,Manjubargavi.A,SanjanaViswanathan and I.Varalakshmi Murugan "Enhanced MANET Data Security againist BOTNET attacks using Hybrid IDS Model".International Journal of Emerging Technology in Computer science and Electronics(IJETCSE).ISSN:0976-1353 volume 12 Issue 2-January 2015.

[3]Kaun-cheng Lin,Sih-Yang Chen,and Jason C.Hung"Botnet Detection using Support Vector Machines with Artificial Fish Swarm Algorithm".Hindawi Publishing Corporation Journal of Applied Mathematics Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 1, January 2014).

[4] Sagar A. Yeshwantrao1, Prof. Vilas J. Jadhav Lecturer, 2Asst. Prof., Department of Computer Engineering,MGM's College of Engineering & Technology Kamothe, Navi Mumbai, State- Maharashtra, Country- India. Threats of Botnet to Internet Security and Respective Defense Strategies. International Journal of Emerging Kyushu University.

[5] Kamaldeep Singh, Sharath Chandra GuntukuAbhishek Thakur, and Chittaranjan Hota Big Data Analytics framework for "Peer-to-Peer Botnet detection using Random Forests". A Department of Computer Science, BITS – Pilani, Hyderabad Campus, AP 500078, India. Information science 2014.School of Computer Engineering, Nanyang Technological University, 50 Nanyang Drive, Singapore 639798, Singapore India,. Information Science 2014.

[6] Pijush Barthakur, Manoj Dalal, Mrinal and Kanti Ghose Department of Computer Science and Engineering Sikkim Manipal Institute of Technology Sikkim, India. "A Framework for P2P Botnet Detection Using SVM (2012)". International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover.

[7] Yao Zhaoy, Yinglian Xie, Fang Yu, Qifa Ke, Yuan Yu, Yan Cheny, and Eliot Gillumz BotGraph: Large Scale Spamming Botnet Detection. Northwestern University Microsoft Research Silicon Valley Microsoft Corporation.

[8]Esraa Alomari, Selvakumar Manickam, B. Gupta,Shankar Karuppayah and Rafeeq Alfaris 3University of New Brunswick, Canada 4RSCOE, University of Pune, India National Advanced IPv6 Centre (NAV6), University Saints

Malaysia, Malaysia. "Botnet-based Distributed Denial of Service (DDOS) Attacks on Web Servers".Classification and Art.) International Journal of Computer Applications (0975 – 8887) Volume 49– No.7, July 2012.

[9] Jingyu Hua and Kouichi Sakurai "A SMS-Based Mobile Botnet Using Flooding Algorithm" Department of Informatics, 2014, Article ID 986428, 9 pages.

[10] James R. Binkley and Suresh Singh," An Algorithm for Anomaly-based Botnet Detection "Computer Science Dept. Portland State University.