Protection Of Critical System From Botnet Based Ddos Attack using Self-Triggered Filters

Dhivyapriya K, L. Kavisankar, Udaya Mouni Boppana, D. Nagarajan

Abstract: ***The motivation of our project is to defend DDOS attack without degradation of network resources and bandwidth. In order to defend DDOS attack, black hole filters are placed in the network, where the inbound or outbound traffic is dropped silently. The black hole filters are invisible, while studying the network topology and can be found only by monitoring the lost packets. There is a technique called remote triggered black filter, that has the ability to discard unexceptionable traffic before it gets entered into the protected area network. But the drawback is, it is located within the premises of victim. So, sometimes the trigger itself gets nonresponsive because of too many packet flooding caused due to DDOS attack. Even if the remote triggers relocate its places in order to avoid the effects caused due to DDOS attack, still the remote triggers are vulnerable as we cannot predict the direction flow of attack packets. So, before degradation of internal network bandwidth, it is necessary to defend the DDOS attack. The triggers that are placed in the network in order to defend DDOS attack, should withstand the effects and impacts caused by DDOS attack. In order to defend DDOS attack, a self-triggered black hole filter should be placed within the control of internet service provider as they have the power to block anything and everything. The self-triggered filters in the network are placed after the proxy server. If there is an anonymity in network behavior like packet flooding, the triggers placed after the proxy server will get self-triggered.***

Keywords: DDOS attack, black hole filter, defending DDOS attack, self-triggered black hole filter, ISP.

I. INTRODUCTION

Among various threats, Botmasters are currently growing threat to confidential organization. Botmasters will create their own army, in which every system will serve as a slave or sleeper cells. Group of slaves or bots form a botnet. Botmasters will control their bot network by command and control server. A bot network consists of infected system called bots, which are responsible for launching attacks on command of botmaster. The botmaster control their bot network through command and control server, which helps in updating and adding new features to bot network. Distributed Denial of Service is one of serious attack down the lane in the history of network security which are carried out by botnets. The main aim of Botmasters are recruiting thousands of bots across the network and managing them. The idea behind managing thousands of bots is to carry out anonymous activities by making use of innocent users across the network. The primary purpose behind the idea is to gather sensitive information for financial gain and survey purpose. Information gathering is carried out to steal confidential data like credit card details, bank account details from the infected users across the network. Aurora was an effective botnet which was mainly responsible for stealing intellectual property information across several organization from different countries [5]. Botnets are responsible for Click frauds that can be achieved by biasing the click status obtained in the popped-up advertisement tabs on the website like online games [6][8]. The goal of Botmasters can be classified as an intentional attack, Entertainment purpose, Personal revenge between large organization. The Fig. 1 explains the life cycle of botnet.

Revised Manuscript Received on May 06, 2019

Dhivyapriya K, Department of Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai, India.

L. Kavisankar, Department of Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai, India.

Udaya Mouni Boppana, Department of Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai, India.

D. Nagarajan, Department of Mathematics, Hindustan Institute of Technology and Science, Chennai, India.

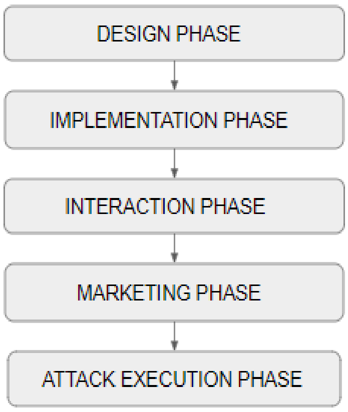

Fig. 1. Botnet Life cycle

The design phase of botnet mainly concentrates on how to infect a system and how to initiate communications among them. The topology of the nodes in bot network can be centralized, distributed or peer to peer based.

Once the designing phase is conceptually designed, **implementation phase** of bot binary code in target system takes place. The target system after execution of bot binary code that has been attached in a fake email or fraud clicks, enters recruitment or infection stage. This is also called as propagation mechanism. The implementation phase is mainly classified into two categories, namely active and passive. In active mode of implementation, the users or human intervention is not required for infecting and locating bots among bot network. It can be achieved by scanning. In passive mode, the implementation of bot binary code is made effective with the help of human intervention. Some websites are especially designed to install bot binary code because those websites are compromised websites.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

These compromised websites are designed with ‘active content’ (JavaScript and ActiveX controls). As a result, these websites initiate automated download of binary code to visiting system [3]. Then comes the **interaction stage**. After executing or implementing bot binary code, the next step is to announce that it is one among the bot network. This is otherwise called as call home process in botnet life cycle. The call home mechanism establishes a connection between the infected system and command & control server through which the infected system receives command and updates [3]. All communication among nodes in bot network operation refers to interaction stage. One of the rock-solid differences between other malwares and bot network is the presence of interaction between them by using C&C messages.

Next comes the **marketing stage**, where the target system joined as one among the army of botnet. Now the botmaster is free to use the target system for launching an attack.

The final stage is **attack execution stage**. The result of botnet is launching an attack. Example is Distributed Denial of Service attack. Now a days, DDoS attack become a serious issue. In DDoS attack, more packets get transmitted in order to flood the bandwidth. Due to a greater number of packets transmitted the data loss becomes high and delivery rate becomes less. The capacity of queue will get exhausted as the packets transmitted exceeds the constant bit rate.

II. RELATED WORK

The Botmaster does not physically own the bot system as the bot systems located across the globe [7]. The connection establishment between two hosts is generalized as a network flow. The combination of five tuple defines the network flow. The source IP address and destination IP address, source port number and destination port number, and protocol defines as tuple. The extraction of information from the network traffic has many ways, one among them is flow extractors. They extract features from 5-tuple such as the flow duration, number of bytes that are transferred in flow [1] etc. The Network based method used to study the network traffic. Depending upon the study, the features can be deployed anywhere in the network topology. Possible locations like proxy server and Internet Service Provider [2]. But some of the Network based bot detection methods leads to degradation of resources and loss of accuracy. The characteristic of network flow extracted from the packet size, interpacket arrival time and the flow duration will get degraded if the bot network manipulates the traffic. Similarly, observation of anomalies in traffic or command and control server degrade if the bot network manipulate the protocol. The behavior analysis of network traffic may include the study of protocol, but it leads to loss of accuracy due to protocol manipulation. The term defensive strategy helps in removal of infection from the infected network. The defensive strategies are classified into two categories as host-based and network based. The host-based method recovers individual machine from bot infection. In host-based method, certain mitigation technique that concentrates on command and control server has no effect for infected bots. The infected bots will continue having negative impact of infection and keeps on participating in malicious activities [3]. The Network based methods, in which once it has come to know that, too many machines started behaving like bot infected machine, it follows two techniques, namely block bots or block command and control communications. By blocking the bots, the networks can be kept secured. The administrations like Internet Service Provider, place the bot infected machine in the administrated network. The Internet Service provider place the infected machine in a state of isolation called walled garden. The infected system joins the network only after it is confirmed as secured and ensures the ISP Policies [4]. There exist most popular DDOS attack tools in order to launch DDOS attack. These tools are designed to launch DDOS attack in both wired and wireless architecture. Some of them are Low Orbit Ion Cannon (LOIC), Trin00, Tribal Flood Network (TFN), Trinity and MStream. Each tool has unique in-built technique. They are unique in terms of encryption technique of channel, architecture and deployment method. But all these tools have same motive, that results in bandwidth wastage and resource depletion [11]. Techniques like Spectral analysis are positive for TCP connection flows. In general, TCP Connection traffic flows are mostly periodic in nature. In connectionless protocols like ICMP and UDP the behavior of periodic traffic flow cannot be predicted, and it is unexpected. So, the attackers make use of this unpredictable situation and tries to confuse the detecting system. [10].

III. ARCHITECTURE OF DEFENCE FOR DDOS ATTACK

DDOS attack is made by bot system to victim system as per the command of Botmasters through C&C Server. Every bot system is connected to command and control server. On command of C&C Server, the bot system launch DDOS attack on the victim system. The victim system can be a large organization’s web server or proxy server. In order to avoid this, a self-triggered black hole filter is placed within the control of internet service provider. The black hole filter, which is placed within the control of ISP, will filter the DDOS attack before attacking the victim’s system.

Fig. 2 Shows the system architecture diagram, in which the self-triggered black hole filter is placed in the network within the control of Internet Service Provider. The filter that is placed in the network will get self-triggered when the number of packets transmitted reaches 1000 in 20 seconds. The length of the packet transmitted is 1024 bytes. The constant bit rate is configured to generate 1Kb packet at the rate of 1Mbps. In general, Internet Service Provider has a blacklist of domain names and IP address. Since the filter is placed within the control of Internet Service provider, the Internet Service Providers keeps on monitoring the flow to ensure whether there is any IP address that matches their blacklist. Additionally, in general, they also check the mapping of source IP address and destination IP address. In usual case, the mapping of source to destination of IP address in DDOS attack will be many to one. Main difference between the flash crowd and attack traffic is, the source IP address of DDOS attack traffic will be distributed geographically across the globe. In DDOS attack, many source IP address targets one victim. Finally, as a result, the self-triggered black hole filter starts filtering the packets with the help of ISP. The victim system is kept untouched and it can withstand the effect of DDOS attack.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The Internet Service Provider supports and controls Quality of Service (QoS), Traffic management etc. Our proposed system extends and add services to the existing techniques of Internet Service Provider, so that the victim system can avoid damage caused by DDOS attack.

.

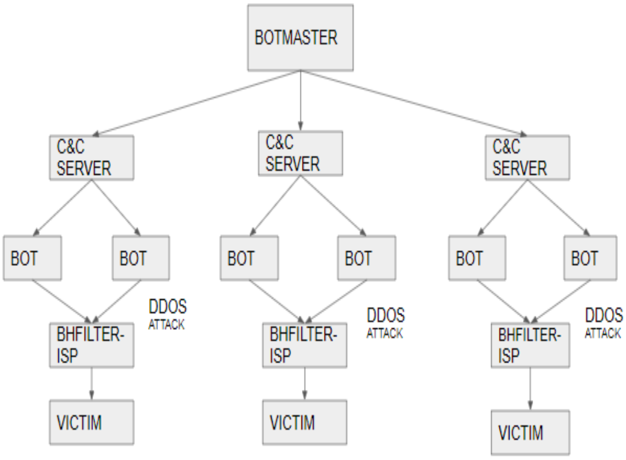

Fig. 2. System Architecture diagram

IV. SIMLATION AND ANALYSIS

In NS2 Simulation, where the nodes represent the systems present in botnet architecture. As shown in Fig. 3, the bot network architecture consists of botmaster, command and control server, bot systems (compromised systems) and victim systems. The figure shows the interaction among the bot systems in bot network as explained in the lifecycle of botnet architecture. We have created one thirty-six nodes. A large network topology in which the command and control server, bot systems are controlled by the botmaster. As shown in Fig. 3, the environment consists of three command and control server through which the botmaster communicates with bot systems. And there are twelve bot systems which are compromised by botmaster. These bot systems are responsible for launching DDOS attack in order to target victim system as shown in figure. 4, and it acts as per the command of C&C Server. The botmaster communicates with the bot system only through C&C Server. And there are four victim system in the setup. These victim systems are assumed to be a large organization's server.

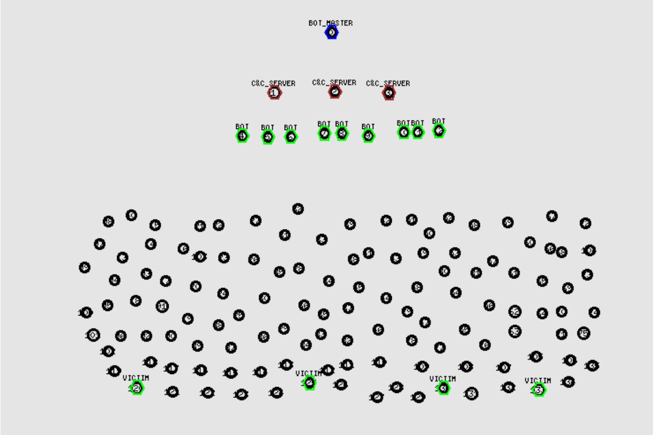

Fig. 3. Nodes in botnet architecture

Now a days, DDOS attack has become a serious issue. In DDOS attack, large number of packets get transmitted in order to flood the bandwidth. Due to a greater number of packets transmitted the data loss becomes high and delivery rate becomes less. The capacity of queue will get exhausted as the packets transmitted exceeds the constant bit rate. In the system architecture, the bot network contains twelve compromised bot system. Among twelve bot systems, four bot systems act as steppingstone to remaining bot system. As we all know the botmaster is seated across several steppingstones of C&C Server, bot systems. The Four bot systems which are labeled in red color as shown in fig. 4, act as attackers. These attackers flood the bandwidth of victim network with packets, which is termed as DDOS attack. DDOS attack generally targets the network bandwidth. [10] The bandwidth attack has two main impacts i.e., consuming maximum amount of host's resources and network bandwidth. Internet Control Message Protocol is an IP protocol in which the network status is diagnosed by ICMP messages. On the other hand, the bandwidth attack uses ICMP Packets to flood the network bandwidth.

V. SIMULATION OF SELF-TRIGGERED BLACK HOLE FILTERS

The black hole filters that are placed in the network, where the inbound or outbound traffic is dropped silently. The black hole filters are invisible, while studying the network topology and can be found only by monitoring the lost packets. The service providers usually flow a technique to filter traffic. The idea behind traffic filtering are, the service providers must define and configure the traffic flow that needed to be discarded. The traffic flow that needs to be discarded based on the configuration and definition of ISP, points to Null0 interface. Null0 interface will discard the packet. There is a technique called remote triggered black filter that can discard unexceptionable traffic before it gets entered into the protected area network [9]. But the drawback is, it is located within the premises of victim. So, sometimes the trigger itself gets nonresponsive because of too many packet flooding. So, in order to avoid this situation, a self-triggered black hole filter should be placed within the control of internet service provider as they have the power to block anything and everything. In simulation, the self-triggered black hole filter is added to the existing techniques and services of Internet Service Provider. Fig. 4. Shows the simulation of DDOS attack and defending strategy.

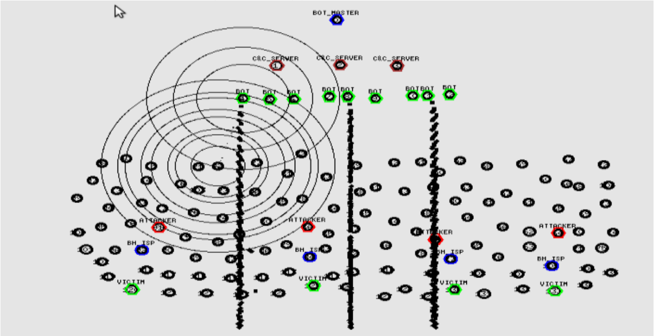

Fig.4 Simulation of DDOS attack with self-triggered black hole filters

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

VI. PARAMETERS USED IN GRAPH ANALYSIS

Table-1 Parameters

Parameters	**DDOS Attack with self-triggered filters**	**DDOS Attack without self-triggered filters**
Throughput	Maximum Throughput rate	Lower Throughput rate
Packet delivery ratio	High packet delivery ratio	Low packet delivery ratio

The throughput of the network is measured in bits per second as an average and sometimes measured as data packets per second. The ration of more unreached message leads to lower throughput rate. The graph compares the throughput with and without a black hole filter that is placed within the control of ISP. Fig. 5. Shows the throughput rate.

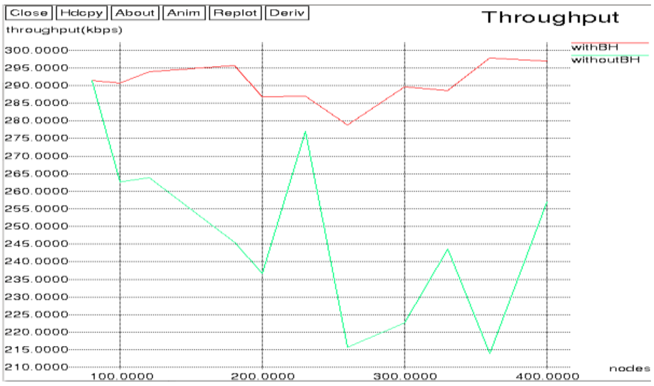

Fig. 5 Comparison of throughput rate with and without self-triggered black hole filters

In Fig. 6, it compares the ratio between received packets at destination and obtained packets in the source with both presence and absence of a self-triggered black hole filter during DDOS attack. As shown in the graph, without black hole filter, the data loss is high due to a greater number of packets transmitted. Delivery rate is less. On the other hand, implementation of self-triggered black hole filter with the help of internet service providers results in less data loss as the bandwidth is not flooded with packets and the delivery rate will be average.

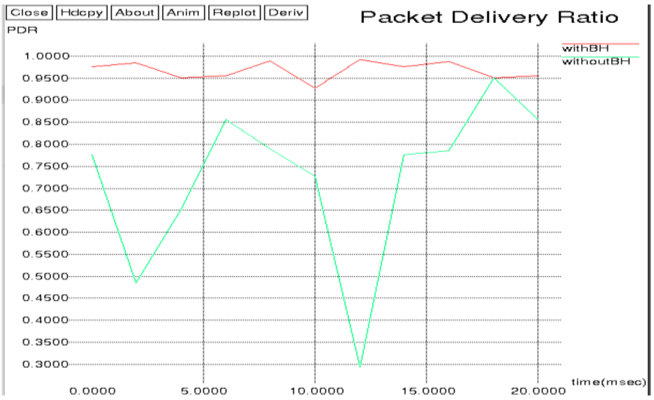

Fig. 6 Comparison of PDR with and without self-triggered filters

VII. CONCLUSION

In order to implement these self triggered black hole filters inside internet service providers all over the world, these providers should have an effective communication between the governments and achieving this is a big challenge. But now a days, DDoS attack has become a big issue that often targets large organizations. So the government should come with an order, that orders internet providers to implement self triggered filters inside their network. "The protection of critical system from botnet based DDOS attack using self-triggered filters" is our proposed work. There are many other threats caused by bot network, but DDOS attack is one of the serious attack among all threats. From our research, we develop a system based on self-triggered filters, that withstand the effects and impacts caused due to DDOS attack. We compared the average throughput rate of DDOS attack without self-triggered filters and DDOS attack with self-triggered filters. The self-triggered filters that are placed in the network, defend the DDOS attack without getting unresponsive. Because of the withstanding nature of self-triggers, the ratio of more successfully reached message becomes high. As shown in the graph, our system withstand the damage caused by DDOS attack . As a result, our system withstand the damage caused by DDOS attack and it enhances the packet delivery ratio and throughput with the help of self-triggered black hole filter.

REFERENCES

1. Pektaş, A., & Acarman, T. (2017). Effective feature selection for botnet detection based on network flow analysis.
2. Karasaridis, A., Rexroad, B., & Hoeflin, D. A. (2007). Wide-Scale Botnet Detection and Characterization. HotBots, 7, 7-7.
3. Khattak, S., Ramay, N. R., Khan, K. R., Syed, A. A., & Khayam, S. A. (2014). A taxonomy of botnet behavior, detection, and defense. IEEE communications surveys & tutorials, 16(2), 898-924.
4. Mody, N., O'Reirdan, M., Masiello, S., & Zebek, J. (2009). Common best practices for mitigating large scale bot infections in residential networks. MAAWG.
5. Lin, S. C., Chen, P. S., & Chang, C. C. (2014). A novel method of mining network flow to detect P2P botnets. Peer-to-Peer Networking and Applications, 7(4), 645-654.
6. Wang, D., Savage, S., & Voelker, G. M. (2013, February). Juice: A longitudinal study of a seo campaign. In Proceedings of the NDSS Symposium.
7. Xie, Y., & Yu, S. Z. (2009). Monitoring the application-layer DDoS attacks for popular websites. IEEE/ACM Transactions on Networking (TON), 17(1), 15-25.
8. Venkatesh, G. K., & Nadarajan, R. A. (2012, June). HTTP botnet detection using adaptive learning rate multilayer feed-forward neural network. In IFIP International Workshop on Information Security Theory and Practice (pp. 38-48). Springer, Berlin, Heidelberg.
9. Sadeghian, A., & Zamani, M. (2014, February). Detecting and preventing DDoS attacks in botnets by the help of self-triggered black holes. In 2014 Asia-Pacific Conference on Computer Aided System Engineering (APCASE) (pp. 38-42). IEEE.
10. Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys (CSUR), 39(1), 3.
11. Nagpal, B., Sharma, P., Chauhan, N., & Panesar, A. (2015, March). DDoS tools: Classification, analysis and comparison. In 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 342-346). IEEE.

AUTHORS PROFILE

K Dhivyapriya, is pursuing her MTech in the Department of Computer Science, Hindustan Institute of Technology & Science, Padur, Chennai. She has done her BTech in Computer Science from SASTRA UNIVERSITY, Thanjavur. Her research interest is Networking, Machine learning, Image processing.

Dr. L. Kavisankar, is working has Associate professor Hindustan Institute of Technology and Science. He was a Research Associate in the Research project “Collaborated Directed Basic Research- Smart and Secure Environment” (CDBR-SSE). The Smart and Secure Environment Research Consortium was funded by National Technical Research Organization (NTRO), Government of India, New Delhi which is used to connect the eight institutions across TamilNadu, India namely IIT Madras, NIT Tiruchirappalli, College of Engineering-Guindy - Anna University, Pondicherry University Pondicherry, PSG College of Technology Coimbatore, Thiyagaraja College of Engineering-Madurai, Madurai Kamaraj University-Madurai, and Alagappa University-Karaikudi through MPLS-VPN network. The worth of the project is nearly 9 crores which were for the duration of 5 years (2007-2012) covering major vulnerabilities with respect to cyber security. He has published research publication in reputed International Journals and Conferences and book chapter. His current research is on IOT, Cyber security, Network security and Computer Forensics.

Udaya Mouni Boppana, is pursuing her MTech in the Department of Computer Science, Hindustan Institute of Technology & Science, Padur, Chennai. She has done her BTech in Computer Science from JNTUK UNIVERSITY, Kakinada. Her research interest is Machine Learning, Image processing, Big data, Networking.

Dr. D. Nagarajan, is a Professor in the Department of Mathematics, Hindustan Institute of technology & Science, Padur, Chennai. He has done his Ph.D. from Manonmaniyam Sundaranar University. His research interests are Stochastic process, Hidden Markov models, Image processing. He is guiding PhD students. He has 50 publications to his credit.