Survey On Botnet Detection using real time packet analysis

Ms. Payal Sondkar[1] , Ms. Snehal Zende[2], Ms. Shital Tamkar[3], Prof.Deepali Lokare[4]
[1,2,3] Research Scholar,[4]Assistant Professor ,ZCOER

Abstract: At present, Botnet is an important demonstration of advanced malware. The botnet is serious threats to our network. Originator(BotMaster) which controls the collection of compromised computers (Bots) from a remote location guided by common command-and-Control(C&C) infrastructure is called Botnet. To convey commands to the bot command and control is used to perform a malicious activity such as sending spam emails, form grabbing, Denial-of-service (DoS) attacks, information capturing etc. Therefore, it is necessary to analyze the botnet to contribute in secure network service.The Proposed work focus on detecting and deactivating Zeus bot, detecting TOR attack and DOS attack and alert to the victim by applying certain steps. To analyze network traffic it is necessary to monitor and observe who is connected to whom and how. The proposed system will give information about Source IP, Destination IP, the name of the protocol, Active Time etc. Based on this information Bots will get detected. The first and second step is to diagnose Bot by monitoring network traffic.

Keywords: Bot, botnet, Communication topologies, c&c server, Zeus, DOS, Tor.

Introduction :

The term botnet is extracted from the combination of ‘robot network’. The bot is designed to perform predefined functions automatically. It creates serious threats to a network asset. Originator (BotMaster)which control collections of compromised computers (Bots) from a remote location beneath a common command and Control(C&C) framework is called Botnet [1]. As shown in fig.1, BotMaster is the computer that attacker used to collect commands which are relayed to the bots through controllers. Once the bot code located into the compromised computers, the computers act as bot or zombie.

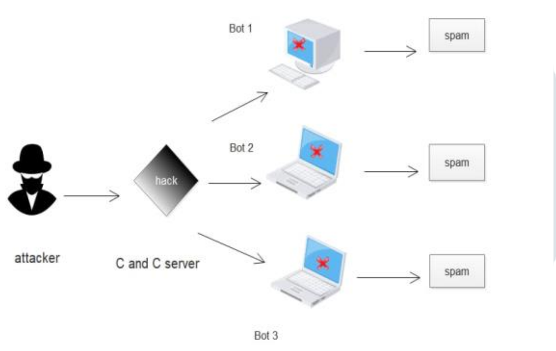

Fig1. BOT networks

The dissimilarity among Botnet, virus, and worm is that botnet has the C&C framework. The C&C permit Bot to receive commands and malicious potentialities through C&C server as devoted by BotMaster. The main goal of malware is attacking and targeting the contaminated host. With respect to the C&C channel, two different models are created which are centralized and decentralized communication model. In Centralized communication model, interchanging commands and data between BotMaster and Bots are accomplish by one central point present in communication [2]. The advantage is that this model has a compact message suspension. The drawback of this model is that, C&C server. If anyone unable to recognize and exclude the C&C server entire Botnet will become ineffectual and incapable. The other communication topology is a decentralized model which does not fail because of a single point lack of success. Therefore, it is difficult to track such type of bot[2].

The botnet is the most prime or dominant threat to the internet. It affects to machine very dangerously under control of the attacker. Hackers are creating own network and control using the Command and Control server. It is not easy to finds causes on the internet by botnets.Various Botnet operating peer to peer networks. Then communication done with server Bots performing tasks such as server send commands and client receives those commands this also avoids the single point of failure. In peer to peer architecture, there is a decentralized point of command and control. There are network nodes perform as both client and server such that there is decentralized coordination that can be in the capacitor.

Here we focus our work on a peer to peer decentralized application, for detection of botnets. Long term goal of our work is to detect botnet and generate the alert. Common action performs by botnets including using your machine assist in DoS attack found, those to shut down websites. Also, generating fake network traffic on the website causes financial gain. Tor another type of botnet those uses hacker for hiding identity. And performing illegal actions and also malicious activities. ZBot is another bot perming malicious actions. ZBot enters to the PC from files such as downloading the file, installing APK, copying files or data from another device then ZBot present in PCs.

Literature Survey:

Network security is becoming a big challenge and issue to professional system developer or organizations. Resources that are vulnerable to malicious activity by attacker need to secure properly. Over the years, the use of the computer system increasing rapidly that is established to the global network. Most of the users must be the perception of external threats and defend them from these threats such as installing Anti-virus, Operating System and Software Patches up to date and also never unsecured e-mail add-on or links etc. From business and organization's point of view, security has greater importance to keep data more secure.

Basil Alothman and Prapa Rattadilok state that Transfer Learning uses separate datasets which are related. The separation is the pivot on the botnet label. For transfer learning Alothman and Rattadilok use the TrAdaBoost algorithm, it endeavors when the source and target task have the comparable arrangement of highlights yet information conveyance is extraordinary. It just improves the execution of models which are utilized for Botnet perceive and recognizable proof [3].

Manoj S.Koli and Manik k.Chavan introduced three new ways for building botnet ID'S for the network. Ranking Feature and Voronoi Clustering techniques are used to remove unnecessary features and to reduce dataset size. The attributes or features of the system stream used to investigate the botnet interruption without being affected by the packet payload content [1].

Priya Mayank and A.K.Singh discussed that generated TLS traffic can be identified, block the traffic a deny access. Also, they found that a script is able to detect Tor traffics in the network and detect Tor IP to which for client wants to communicate. They also focus on onTLS handshake implementation of Tor and other TLS services [4].

Guofei Gu et.al[5] states bot inside comparative botnet will publically show comparative C&C correspondence and pernicious exercises designs. Botminer is to detect already compromised machines within the observed network that are part of a bot network. Botminer does not detect botnet at the very moment when victim machines infected with malware. Its drawback is Traffic randomization and mimicry, Individual or group commands, delay not tasks [5].

Piyush Goyal and Anurag Goyal .discussed about Wireshark. Wireshark is a packet analyzer, among different network interface which catches and analyze live packet data. Wireshark will show that packet data in detailed or fact as possible. Wireshark is not an IDS system. It will not alert you when someone does malicious on your network. However, if malicious activity happens, Wireshark helps you find out what is really going on [6].

RaviTeja Gaddam and Dr. M. Nandhini state Snort is a free open source system created in 1998 by Martin Roesch. It is an interruption counteractive action framework and system interruption discovery framework. It takes a shot at parcel logging and continuous traffic examination on systems. Snort uses a rule-based intrusion-detection mechanism for detecting potential network intrusions. Snort uses packet sniffing mode to capture and display network traffic and creates the traffic data file [7].

Drawback:

1) The system will be much less efficient because of Snort missing attacks completely if Snort system with rules not updated properly.
2)Snort is only working on its defined rule set, it does not have the ability to tell which traffic is considered to be normal and seems to be out of place from each host on the network.

BotSniffer is a system contamination based botnet identification framework. It navigates similitude properties of botnet direction and control exercises and it distinguishes bot C&C divert in LAN. BotSniffer depends on perception it is effectively distinguished the correlations among bots inside the same botnet. It has low FP(false positive) rate and uses several correlation algorithms [8]

Disadvantage:

1) If botnet traffic is normal, it cannot detect.
2) It is detected only IRC and HTTP.

Abdulaziz Aborujlah, Miss, Shahzad, Nasti states that to recognize flooding based DoS attack future subset selection (FSS) algorithm can be used. It selects less related features from the dataset, no real experiments done. By integrating these selected features into classification method such as KNN performance can be validated. The goal of this system is to improve the accuracy of intrusion detection system but there are some issues to achieve this [9].

Hossein Rouhani Zeidanloo, Azizah Bt Abdul Manaf states that the system focuses on p2p and ORC based Botnet. Collection of bots(infected machines) that will cause similar communication and malicious activities within similar Botnet is called P2p Botnet. It improves the efficiency of a framework by adding more unique recognition technique in Http part. P2p Botnet detection removes and hides the central point of failure which is a drawback of centralizing model [10].

Proposed System:

The drawback of traditional perspective is that data is costlier and difficult to obtain. The quality of botnet detection will not perfect by using a small amount of data. In the second approach every time it is not satisfactory to binned datasets which accommodate network traffic from various kind of Botnets. In Proposed system instead of concatenating datasets, proposed work is mainly focused on live packet capture. It will detect victim machines within a monitored network that are part of a botnet at a time that occurs. This can be done by using network monitoring technique.

In the proposed system, the Jpcap Java library is used which capture and send network packets. It deals with any OS that conveys libpcap/winpcap and it additionally bolsters Ethernet, IPv4, IPv6, ARP/RARP, TCP, UDP, ICMPv4 parcels. Utilizing Jpcap for programming it is doable to catch and assemble the system information bundle, and after that perform an investigation and the measurements. It can set the required catch channel which diminishes the framework load as indicated by interest.**System**

Architecture :

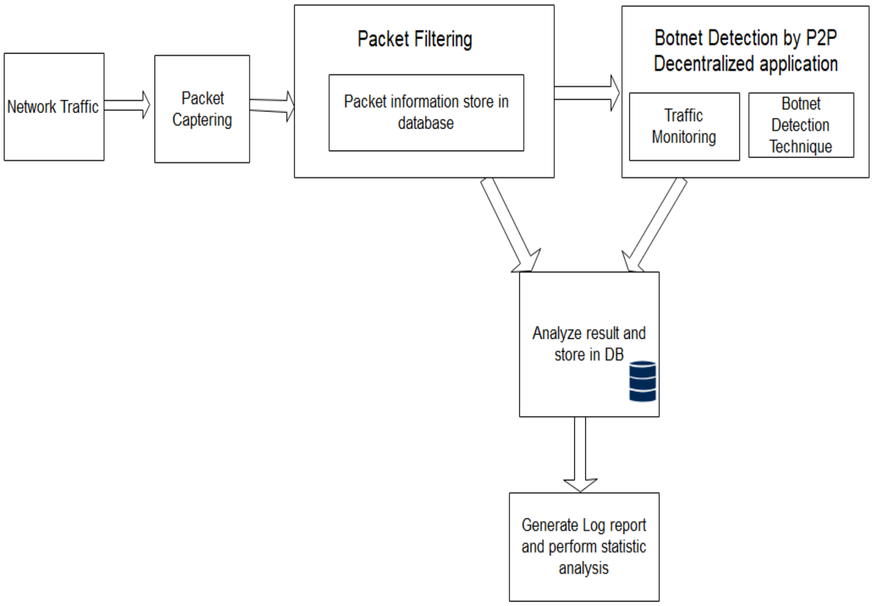
Network Traffic
Packet Captering
Packet Filtering
Packet information store in database
Botnet Detection by P2P Decentralized application
Traffic Monitoring
Botnet Detection Technique
Analyze result and store in DB
Generate Log report and perform statistic analysis

Fig.2 System Architecture

According to System architecture given in Fig.2 Working of Proposed system is as follow:

Network Traffic: Network traffic is the flowing data or moving data across the network at the point of time. Transmitting packets over the network. These packets consist of a header of packet and data payload. packet header manager Prepare and maintaining the list of protocol which is active in nature. And data payload store actual data. Network traffic monitoring by tacking response time of access points such as router and server on the network. Security is important for networking area. Network security uses an overall analysis of network traffic to find out malicious and suspicious packets within the network. Analysis of network traffic also used by hackers or attackers for finding or identify patterns of network traffic and vulnerabilities that means to break in or retrieving sensitive information.

Packet Capturing: Small subdivisions of data called as packets are routed in the network by way of the internet. Routing of this packet depending on the destination address carried within each packet. These packets are reassembled in such a way that it reaches the target destination address. When a packet sniffer enters in the network, which intercepts the network traffic and capture packets. Packets Capture is the activity of intercepting and logging traffic.

Packet Filtering: Packet filtering control the data can flow to and from a network, it is a network security mechanism. Packet filters examine only the header of the packet. The main purpose of Filtering is to overcome traffic load which helps the network system to work well organized.

Network Traffic Monitoring: Network Traffic Monitoring is the process of network monitoring technique which identifies the victim machines that are part of the botnet at the time of victim machine get targeted.

Botnet detection or malicious activity detector: It analyzes the network traffic and detects the victim machine within the network. After detecting the victim machine within the botnet give an alert to the user.

Result analysis and store in database: In this stage records regarding packet filtering, traffic monitoring, source, and destination IP address are stored in the database.

Generate log report: We can perform analysis on the log report generated.

Conclusion and Future Scope:

The threats to the Internet can be viruses, worm, and bots that perform malicious work. These impacts both network and personal computers. The impact of attacking personal computers may corrupt the user's computers or steal information. The proposed framework depends on peculiarity based bot acknowledgment technique which is utilized to dissect bot from the injured individual machine to contribute to secure system administration. Traditional machine learning algorithm uses dataset separately to create a predictive module which needs data pre-processing. In the proposed system JPCAP library is used to capture the real-time network traffic and it also analyzes the protocol. The drawback of the traditional system which performs analysis on stored dataset so it is difficult to alert the victim machine within botnet at the time system gets targeted. Proposed System will solve this problem. In the future, we can work on all types of botnets.

References:

[1] 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)

[2] Hossein Rouhani, Azizah Bt Abdul Manaf," Botnet detection by monitoring similar communication pattern". IJCSIS, Vol. 7, No. 3, 2010

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

[4] Priya Mayank and A. K. Singh "Tor Traffic Identification", 2017 7th International Conference on Communication Systems and Network Technologies

[5] Guofei Gu, Roberto Perdisci , Junjie Zhang , and Wenke Lee " Botminer: Clustering Analysis of Network Traffic for protocol and Structure- Independent Botnet Detection", 17th USENIX Security Symposium

[6] Piyush Goyal, Anurag Goyal "Comparative Study of two Most Popular Packet Sniffing Tools - Tcpdump and Wireshark ." , 2017 9th International Conference on Computational Intelligence and Communication Networks .

[7] RaviTeja Gaddam and Dr. M. Nandhini "An Analysis of Various Snort Based Techniques to Detect and Prevent Intrusions in Networks ", International conference on Iventive Communication and Computational Technologies(ICICCT 2017).

[8] Jhilam Biswas , Ashutosh " Bot Sniffer : An Insight in to Network Traffic Analysis using Packet Sniffer ",International Journal of Computer Applications (0975 – 8887) Volume 94 – No 11, May 2014

[9] Abdulaziz Aborujlah,Miss,Shahzad,Nasti "Flooding based DoS Attack feature selection using Remove Correlated Attributes Algorithm"

[10] Hossein Rouhani Zeidanloo, Azizah Bt Abdul Manaf "Botnet detectipn by monitoring similar communication patterns"

[11] https://github.com/jpcap/jpcap