International Journal of Engineering Trends and Applications (IJETA) – Volume 2 Issue 2, Mar-Apr 2015

RESEARCH ARTICLE OPEN ACCESS

A Proposed Algorithmic approach of Bot-Matrix Propagation in Botnet Detection

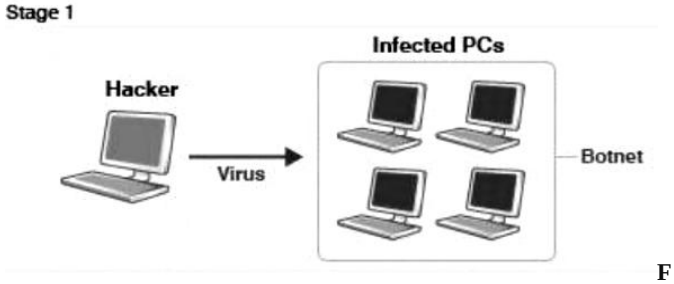
Bidyutmala Saha [1],Santanu Kumar Sen [2], Debraj Roy [3]
Sandip Tigga [4], Sourish Mitra [5]
Department of Computer Science and Engineering
Gurunanak Institute of Technology
Sodepur, Panihati, Kolkata
West Bengal - India

ABSTRACT
The term "Bot" refers to an infected computer that takes order and reports back. Botnet is a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam. More specifically a botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. Now a days in case of network security botnet detection becomes a challenging work and it makes easier for intruders and attackers to generate attacks. Due to the concept of centralized propagation, botnet floods infectious hazards through different botnet clients inside the network and then network security becomes hampered. To overcome the challenges in identifying the botnet, we propose a new modified propagation algorithm for botnet detection. Our proposed method keeps track the signature of identified infectious hazards and also listed out different hops that traversed through a path. In this algorithm each hazard signature becomes identified and then we can be able to maintain a matrix which contains bot elements, in which set of hop addresses traversed by the data packet is stored. That's why when any infectious packet is identified inside the network, different visited hop addresses are identified in its traversal path and after comparing it with the list of hops present in the bot matrix we can be able to provide far better security of that network.
***Keywords*:-** Bot, Botnet, Internet Relay Chat, Infectious hazards, Centralized propagation, Botmatrix.

I. INTRODUCTION

A 'bot' is a type of malware that an attacker can use to control an infected computer or mobile device. A group or network of machines that have been co-opted this way and are under the control of the same attacker is known a 'botnet'. Bot programs can be planted on a machine or device in many ways. Machines or devices that have been infected by a bot are sometimes called 'bots' themselves, or 'zombies'. One common method for a bot program to get on a machine is when a harmful website the user is visiting silently looks for and exploits vulnerability in the user's system to install the bot on it. Other popular ways include sending the bot as a file attached to spam emails sent to the user, or as a program dropped from the payload of another malware. Once the bot program is installed on the device, it will try to contact the website or server where it can retrieve instructions from the bothered. This site or server is known as the command-and-control (C&C) server. An attacker with access to the C&C servers uses a client program to silently send instructions over the Internet (or another network) to the bot to perform various tasks, such as collecting data, monitoring the user's actions and so on. Commands can be issued to a single bot, or to all the bots in botnet. The attacker controlling the botnet is Sometimes referred to as the 'bothered', 'operator' or 'controller'. Botnets can cause significant damage to the security of both individuals and businesses. Most directly, the data and connected resources of any systems forced into a botnet are no longer under the legitimate user's control. Most people today store highly sensitive content on their personal machines, such as financial accounts, login credentials, etc.; on an infected system, this data can be easily harvested by the attackers. If the enslaved machines belong to a major corporation or government organization, this puts critical business functions or social services at risk. For example, back when the Conficker botnet was active, there were reports that among all the personal home computers roped in, military resources in the United States, the United Kingdom and France were also infected and were forced to take significant remedial actions because of security concerns. Conficker also had a disproportionately large effect on the Internet infrastructure of entire developing countries, in many cases severely disrupting businesses and home users in the affected nations. Attackers can also use the collective resources of all the machines in a botnet for their own activities. These include: launching Denial of Service (DoS) attacks on

websites or services; sending out spam emails or malware; or mining digital currency, such as Bitcoin. Botherders can also sell the use of 'their' botnets to others who want to perform these activities, or sell the botnets outright. In recent years, botnets have become more 'commercialized' and are increasingly used by crime syndicates to perform data theft, fraud and other harmful activities. When we want to discuss about the working procedure of botnet then we must have to seperate the process into two corresponding stages. In first stage, a hacker sends out a virus or worm over the internet to infect vulnerable home computers. This creates a network of slave machines known as botnet.



F ig-1. Stage-1 working procedure of botnet

In next stage of the working procedure of botnet, the hacker sales or hires out the botnet to other criminals who use it for fraud, spamming, Distributed Denial of service attacks and other cyber crimes.

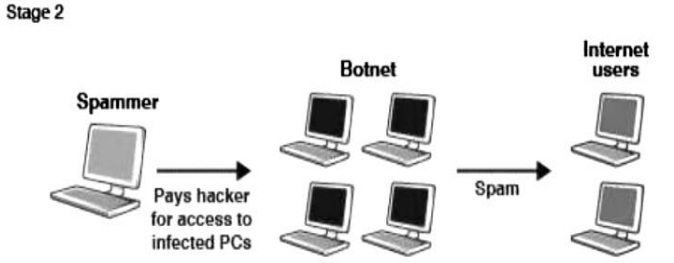


Fig-2. Stage-2 working procedure of botnet

Once botnet infects a computer, a bot usually steals something such as personal information, authentication credentials or credit card data. The machine then becomes part of the botnet, ready to perform designated malicious tasks. Common functions in most botnets include DDOS attacks, click fraud, spam, phishing etc.

II. LIFE CYCLE AND ARCHITECTURE OF BOTNET

Bot usually refers to software robots, which are used to automate tasks. Nowadays bot refers to an infected compromised computer which can accept commands from remote controller (bot master). Botnet is a network of infected systems under the control of a bot master. The bot master can perform coordinated activities with these bots by issuing commands. In recent times, use of bots for nefarious activities poses serious threat. They are used for a) Distributed Denial of Service attacks b) Spamming c) Click Fraud, d) Spyware.

A. LIFE CYCLE OF BOT:

The life cycle of an IRC based bot is explained as follows. It begins with the infection stage. The exploitation of victim computer can be due to any one of the following reasons.

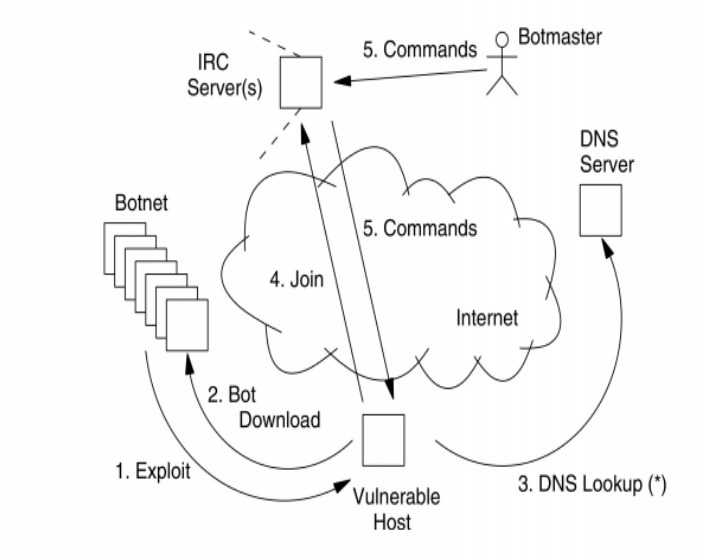


Fig.3. Life cycle of Bot

a) Unpatched vulnerabilities. b)Backdoors left by trojans. c)Password guessing and brute force attacks. The infected machine is called a zombie or a drone. Once a host is infected, it downloads the bot binary source from a remote server and installs automatically. The bot then looks up for the address of IRC servers by DNS Lookups. These IRC servers are called Command and Control (C&C) servers. On obtaining the C&C server's address, the bot then logs into it and authenticates itself as a part of the particular botnet. The bots can then update their bot software, this is usually functionalities added to the bot software, if an update were available and add more C&C servers. IRC servers are used for C&C by bot masters is due to the following reasons. a)Easy to install i.e. private network can be installed easily. b)Easy to control i.e. using features like username, passwords.

Most botnets that have appeared until now have had a common centralized architecture. From a botmaster's perspective, the C&C(Command &Control) servers are the fundamental weak points in current botnet architectures. Because botmaster will lose control of their botnet once the limited number of C&C servers are shut down by defenders.

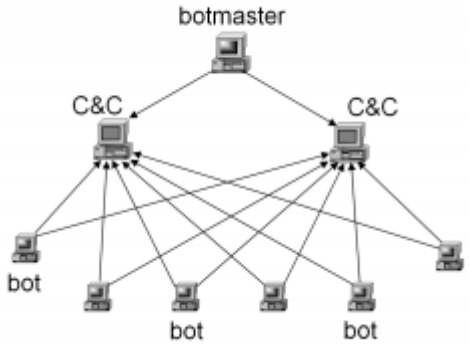
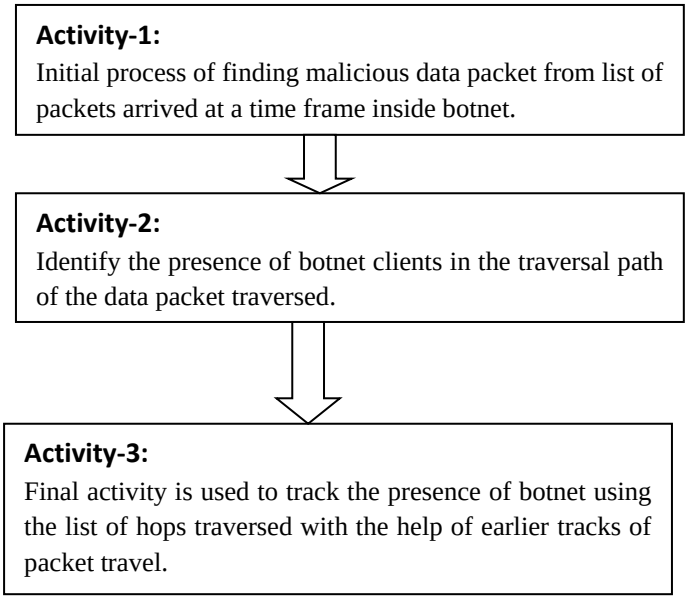


Fig. C&C architecture of C&C- Botnet

Then an entire botnet may be exposed once a C&C server in the botnet is hijacked or captured by defenders. That is, bots in the botnet connect directly to some special hosts (called "command-and-control" servers, or "C&C" servers). These C&C servers receive commands from their botmaster and forward them.

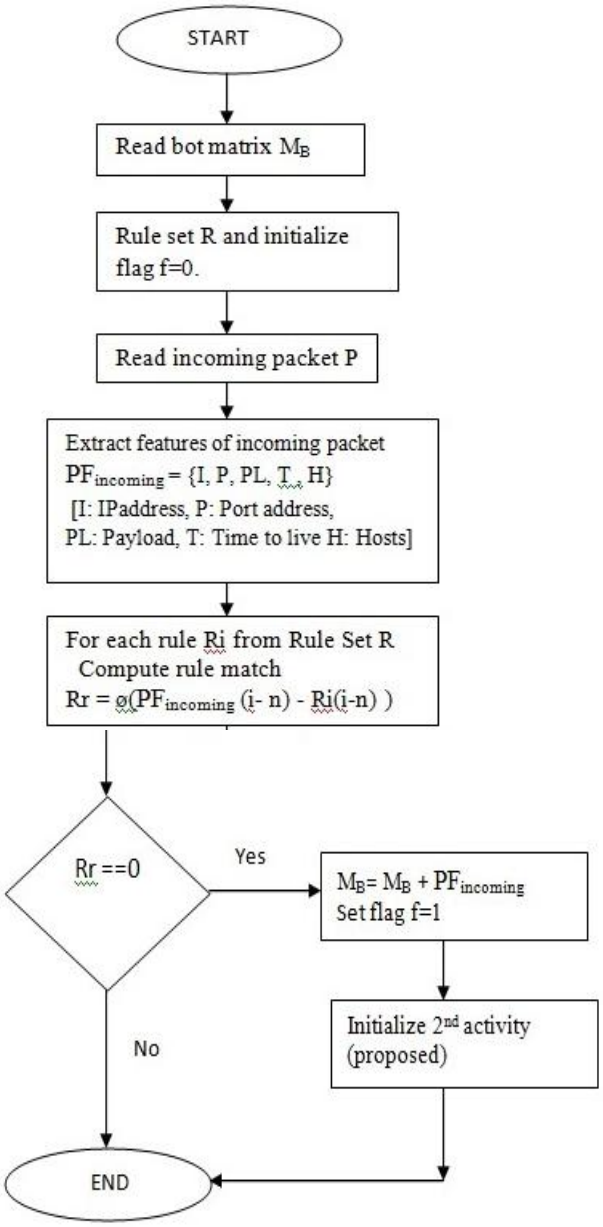
III. OUR PROPOSED WORK

Our proposed model has three operational activities.



A. PROPOSED ALGORITHM FOR ACTIVITY-1

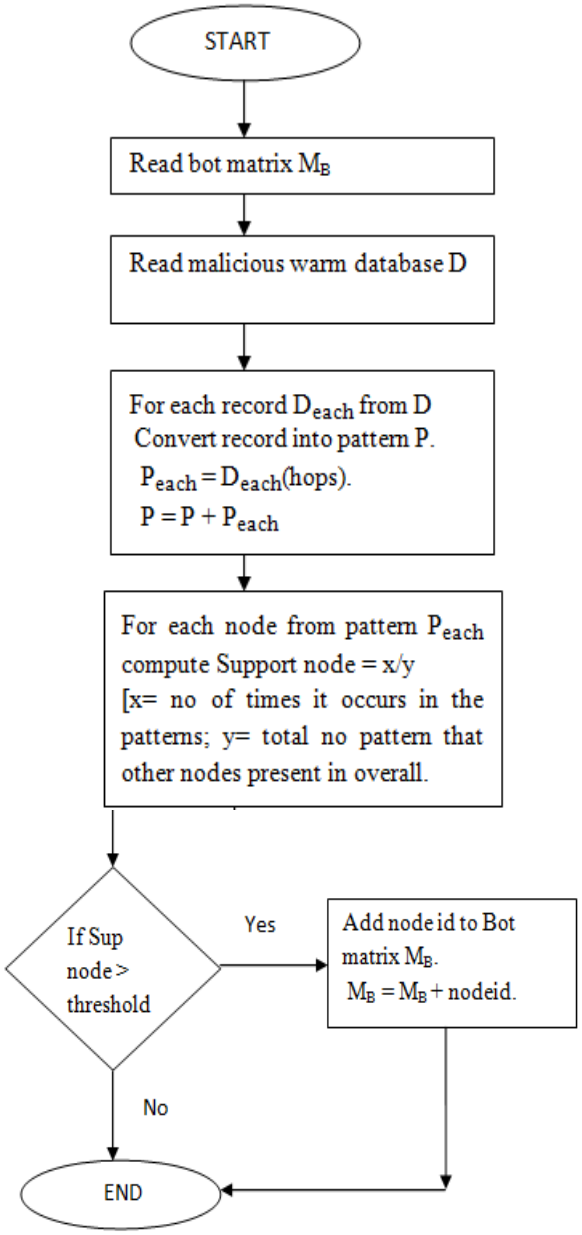
Our proposed algorithm is designed for identifying malicious data packets which are incoming into the network. This functional model is capable of identifying and classifying the packet into various attacking type. It uses set of rules to identify the packet type and if any of the rules matches with the signature of the packet then it will assign the flag to the packet received.



B. PROPOSED ALGORITHM FOR ACTIVITY-2

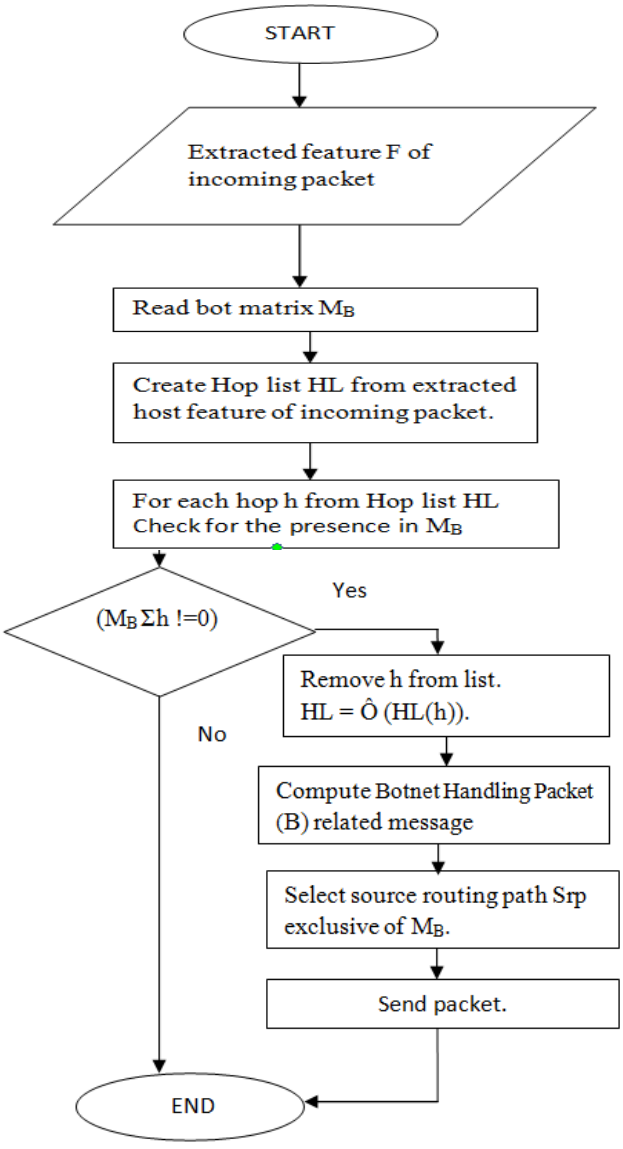
Whenever a warm identified by the system it stores the whole packet features to the data base. From the store data we extract the common pattern or frequent pattern present in the traversal path is identified. We compute the sub set of patterns and compute the frequency of each subset of pattern. The patterns which have more support value is identified as the members of

botnet or botnet clients. The occurrence of a node in more traversal path shows definite guilty.



C. PROPOSED ALGORITHM FOR ACTIVITY-3

The identified malicious packet details will be the trigger to invoke this functional model. The extracted packet feature and bot matrix is used to traverse the source of spam from where it injected into the network. Once its feature is identified and the proposed system generates a Botnet Handling Packet (B) and sends the packet to the source node. While forwarding the packet it uses source routing mechanism, so that the packet path can be predefined. The selection of path to be traversed by the B packet is done using the bot matrix M_B. From the packet feature of the received packet it extracts the list of hops and for each hop from the traversal path it check for the occurrence in the bot matrix. Once it has an occurrence in the bot matrix the hop id will be removed from the list. Finally it selects a different path which does not pass through any of the node from bot matrix.



IV. EXPERIMENTAL ANALYSIS

The proposed propagation model has been implemented in Network simulator Ns2. It produced efficient results and the identification of botnet has performed efficiently. It is clear that the detection accuracy and frequency is increasing

according to the number of warm packets received. The proposed system is a learning system so that if the number of spam packets received is increases then the frequency of botnet detection also gets increased.

V. CONCLUSION

Our proposed approach has produced very efficient results. As the warm data base increases the size of bot matrix also gets increased. This helps the proposed system to identify more botnet clients and botnet nodes. So that the packet delivery and throughput of the overall network gets increased. Our proposed work helps the peer to peer networks to identify the botnet nodes efficiently and it makes easier to send data packets in some other way to overlook the botnet nodes.

REFERENCES

[1] G. Gu, J. Zhang, and W. Lee, "Botsniffer: Detecting botnet commandand control channels in network traffic," in Proc. 15th Annual Networkand distributed System Security Symposium (NDSS'08), 2008.

[2] A.Ramachandran, N. eamster, and D.Dagon, "Revealing BotnetMembership Using DNSBL Counter-Intelligence," Proc. USENIXSecond Workshop Steps to Reducing Unwanted Traffic on the Internet(SRUTI '06), June 2006.

[3] Arce and E. Levy, "An Analysis of the Slapper Worm," IEEESecurity & Privacy Magazine, vol. 1, no. 1, pp. 82-87, Jan.-Feb. 2003

[4] T.Strayer,"Detecting Botnets with Tight Command and Control,"ARO/DARPA/DHS Special Workshop Botnet, 2006.

[5] Y. Chen," IRC-Based Botnet Detection on High - Speed Routers,"ARO/DARPA/DHS Special Workshop Botnet, 2006.

[6] Peer File-Sharing Technology: Consumer Protection and CompetitionIssues," Federal Trade Commission Report, June 2005.

[7] S.H. Kwok, "Watermark-Based Copyright Protection SystemSecurity," Comm. ACM, pp. 98-101, Oct. 2003.

[8] G. Pallis and A. Vakali, " Insight and Perspectives for ContentDelivery Networks," Comm. ACM, pp. 101-106, Jan. 2006.

[9] P.Rodriguez et al ., " On the Feasibility of Commercial Legal P2PContent Distribution," SIGCOMM Computer Comm. Rev., vol. 36,no. 1, pp. 75-78, Jan. 2006.

[10] C. Livadas, R. Walsh, D. Lapsley, and T. Strayer, Using Machine Learning Techniques to Identify Botnet Traffic," Submitted to 2nd IEEE LCN Workshop on Network Security, 2006.

[11] B.Saha and A.Gairola, "Botnet: An overview," CERT-In WhitePaperCIWP-2005-05, 2005.

[12] J. R. Binkley and S.Singh, "An algorithm for anomaly-based botnetdetection," in Proc. USENIX Steps to Reducing Unwanted Traffic on theInternet Workshop (SRUTI'06), , 2006, pp 43–48.

[13] Karasaridis, B. Rexroad, and D. Hoeflin, "Wide-scale botnetdetection and characterization," in Proc. 1st Workshop on Hot Topics inUnderstanding Botnets, 2007.