METHOD FOR IDENTIFYING AND MITIGATING BOTNET ATTACKS

M Hariharan[1], M Mohamed Mufazil Lebbai[2], A Mohamed Musthafa[3]
[1,2,3]Department of Computer and Engineering, Thiagarajar College of Engineering, Madurai
Email: hariinfo04@gmail.com[1],mufacse@gmail.com[2],musthafatce@gmail.com[3]

Abstract
Botnets have become a major engines for malicious activities in cyberspace nowadays. For a successful Distributed Denial of Service attack, a bot master must ensure that all the bots that are in the part of a botnet is intact. To ensure that the bots are alive, the bot master checks the activeness of every bots in its network by establishing IRC server client communication and asks for its host identity and details. We try to monitor every system in our network for bot activity. If it transfers any suspicious data over the network to any suspicious websites then we isolate the bot and close its port. Now for the bot master to successfully carry out his attack he must ensure all the bots to be active. So he sends another bot to open the port or in the best case the bot master may itself comes to open the port. By this we can prevent Distributed Denial of Service attack as well as find a bot that tries to force open the port.
Keywords: Botnets, Denial of Service, Port Closing, Mitigation

I. INTRODUCTION

Botnets are the main drivers of cyber attacks, such as distributed denial of service (DDoS), information phishing and email spamming. These attacks are pervasive in the Internet, and often cause great financial loss[1],[2].Motivated by huge financial or political reward, attackers find it worth while to organize sophisticated botnets for use as attack tools. There are numerous types of botnets in cyberspace, such as DSNXbot, evilbot, G-Sysbot, sdbot, and Spybot [3]. On one hand, researchers have studied botnets from various perspectives, including botnet probing events [4], Internet connectivity [5], size [6], and domain fluxing [7], [8]. On the other hand, botnet owners have at their disposal state-of-the art techniques, such as stepping stones, reflectors, IP spoofing [1],[9],code obfuscation, memory encryption[10],and peer to peer implementation technology[9],[11],[12] to sustain their botnets and disguise their malicious activities and traces. However for every type of attacks to be successful every botnet owner must ensure that all the bots in their disposal are active to carry out their DDoS attack. For this the bot master checks the activeness of every bot by sending keep alive message. So in this paper we try to find the bot which acts as a intermediary to carry out the botnet attack by closing the port through which it communicates with the bots that are to be involved in a botnet attack by closing their respective ports . By closing their ports the intermediary bot tries to forcefully open the port and communicates with it. This intermediary bot identity can be noted now for preventing future attacks and communication with the bot.

II. LITERATURE REVIEW

A. Fool Me If You Can: Mimicking Attacks and Anti-Attacks in Cyberspace

Shui Yu in their paper proved that legitimate cyber behavior can be successfully simulated, therefore, it is not possible to discriminate mimicking attacks from legitimate cyber events using statistical methods. However, in order to achieve this, attackers need to satisfy one critical condition: they have to possess a sufficiently large number of active bots, with no fewer than the number of active legitimate users

of the simulated events. By active bots, we mean the bots that botnet owners can manipulate at the time they initiate attacks.

B. Wireshark network analysis: the official Wireshark certified network analyst study guide

Laura chappell of wireshark university has showed some methods for identifying bot activity by monitoring the bot closely and observing the data and system behaviour. We implement those methods in identifying the bot in our network by following her methods proposed.

III. EXPERIMENTS OVERVIEW

A. SETTING THE REQUIRED ENVIRONMENT

For setting a bot compromised system we setup a batch script that pings the network over a definite interval which we consider the pinging situation as bot to bot communication. The bot may try to ping the network for any sites in our scenario and ensures that the system is active. This is the same scenario in a bot infected environment which tries to communicate with the intermediary bot or bot master. Over some definite period of time the bot sends the system‟s id and other sensitive information over the network to the intermediary bot. This activity of the bot over the network is sniffed by using the tool wireshark. Wireshark provides necessary functions to sniff the network over Local Area Network , Wi-Fi, Bluetooth network. We can follow the TCP stream of the bot that communicates with the network using wireshark.

B. MONITORING THE NETWORK

After setting up wireshark we can now sniff the network and look up for any suspicious activity that happens between the systems and destined system over the network. For sniffing the network open the wireshark tool with administrator privilege and choose the respective connection of the network which may be Local Area Network , Wi-Fi, Bluetooth network. Now after selecting the network wireshark starts to capture packets that are transferred to and from the network. It also gives us the time, source and destination ip, length of the packets, port with which it communicates, TCP handshakes, protocol used and also the details regarding the packets. If a bot activity is detected, the data packets transferred to and from the designated bot can be monitored much more closely and effectively by using the „follow TCP stream‟ function provided with the wireshark tool. This option lists the data and its information only between the two systems.

C. IDENTIFYING THE BOT

A system in our network is assumed to be compromised as a bot. This bot infected system is stimulated by running a batch script in a system that pings the network over a definite interval . It is similar to a bot that responds to the keep alive message issued by the bot master or any intermediary bot to check its activeness. A bot can be distinguished from any other legitimate system by checking the data stream of every systems in the network. A bot tries to resolve a domain name to a set of IPs and the bot establishes a TCP handshake with any one of the returned IPs. A suspicious domain name can be distinguished from a legitimate one when the domain name resolves to more than five IPs as proposed by Laura chappell from wireshark university. The domain name is thus further cross checked for its reliability. If the above symptoms is observed then the system‟s activity is closely monitored by following its TCP stream as mentioned above. Now the data transferred between the two systems is listed in a new window. If the host sends any suspicious data like user id, name, sensitive information to the malicious designation then the host can be regarded as a bot. When analyzing the data packets transferred the host may try to send user information or any suspicious information by using PUSH [PSH] by which it avoids storing the data in the buffer. This way the information is avoided from storing locally and transferring directly. The bot can be identified as sending sensitive information by noting the commands like User, USeRHOST, JOiN. These are the commands which gets specific user related information when the bot connects with the Internet Relay Chat (IRC) or any other webservers to control the botnets.

D. CLOSING THE SUSPECTED PORT

After monitoring the systems in a network we find that one or more systems is compromised as bot and then the port through which the bots that are responding to the keep alive messages and sending sensitive information over the network is noted using wireshark tool. Now we have the ports of all the bots which are suspected to be

involved in a botnet so the next step is to close all the suspected ports for preventing further communication between bots. The ports can be closed by using TCPView software by Microsoft by which we can close the ports of the bots by having administrator privileges. After closing all the ports, the bot cannot communicate over the network and cannot respond to its keep alive messages.

E. FORCE OPENING OUR CLOSED PORT

Now that the communication between bot and intermediary bot has been cut off. The intermediary bot now tries to communicate with the bot to check its activeness. But the bot doesn‟t respond because the port through which it communicates is blocked. So the intermediary bot tries to force open the port and tries to reestablish its connection with the bot. This port opening can be observed through our wireshark tool where we can see that the bot regains its access to the other bot and responds to its keep alive messages and typically breaches our security.

IV. METHODOLOGY

The methodology followed in our paper involves checking our computers network for any bot compromised system by following our proposed methods isolating and keeping constant checking of the data transferred between the system and the destined bot. Then closing the suspected port and preventing further communication with the intermediary bot and checking if the port is being force opened and resuming the data transfer with the designed bot.

The environment should be set up in prior to detecting and preventing bot attacks by setting up the tools for observing the network and data transferred between systems and tool for stopping the port from further data transfer.

Below mentioned tools are required to be installed in the environment for carrying out our methodologies.

- Wireshark- for monitoring the network and observing the data packets transferred between the host and destination.

- TCP View- closing the port in which the host and destination is communicating.

The Figure 1 describes the methodology used in identifying and isolating bots and preventing them from further communicating with botmaster and intermediary bot.

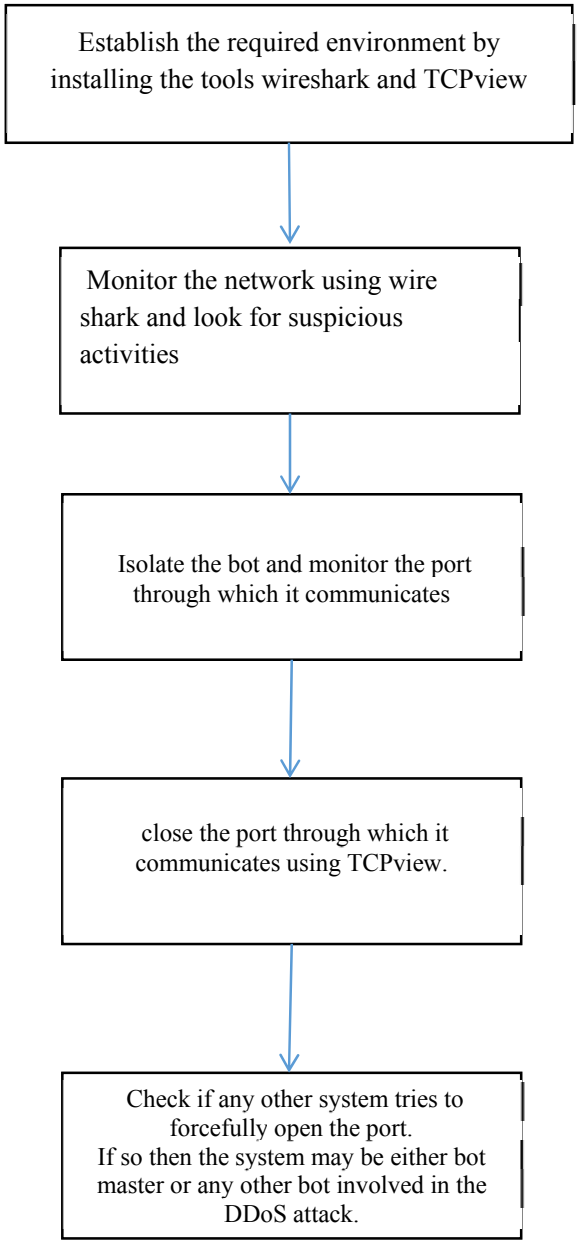

Fig 1. Methodology used in our method for mitigating botnet attack

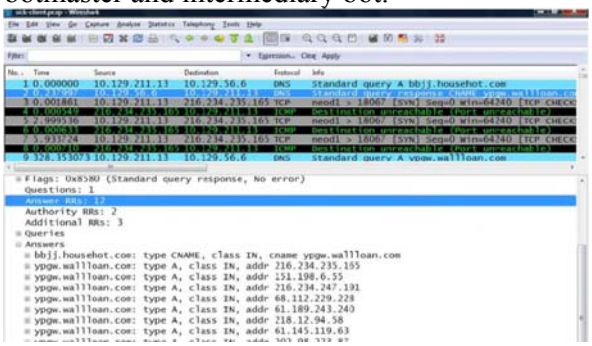

Fig 2. DNS resolved to more than 5 IPs

The Figure 2 of our experiment shows that the domain name resolved has provided multiple IPs in which the Answer RRs has exceeded 5. This

observation clearly shows that the system under observation is a bot and connecting with malicious websites.

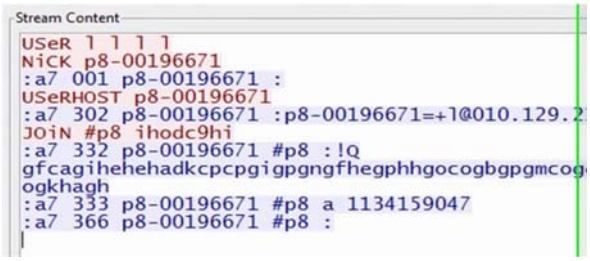

Fig 3. TCP Data stream of bot with destination

The Figure 3 describes the TCP Stream followed from the bot and it can be observed that the bot tries to send user ID by using the USER and USERHOST commands and requests for joining the IRC server by using the JOIN command for establishing a connection with the host and destination.

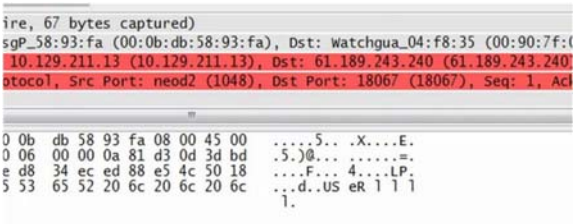

Fig 4. The intermediary bot asks for user details

The Figure 4 shows the activity of the bot observed when it opened the closed port and requesting for user details for maintaining its activeness with the destined bot and it can be identified by observing the data packets.

V. RESULT

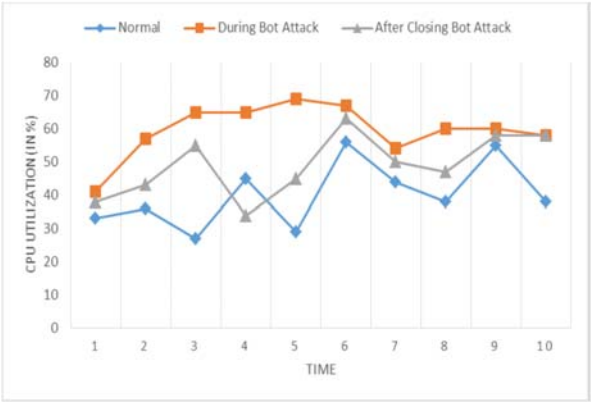

Fig 5. Graph depicting the CPU utilization under normal state, bot infected state and final state after stopping bot activity

The Figure 5 depicts that the CPU resource utilized by a bot is higher than that of the CPU resource utilized by our system under normal condition. So after identifying and stopping the bot activity using our proposed method, the system resource utilization has now become normal and it correlates with that of the usual system behavior thus mitigating the bot activity.

VI. CONCLUSION

The intermediary bot id and its information can now be noted and can be now blacklisted. So in the future when some other system accesses the intermediary bot then the access can be prevented by verifying our blacklist. In this way we can effectively prevent DDoS attack by preventing a bot to reestablish its connection and preventing future communication with the botnet. However in some special cases the bot that is under observation maybe the endpoint system in the botnet which is required for DDoS attacks. In that case the bot master may not risk into retrieving the bot into its network. But that is the worst case scenario and its can also be neglected because whenever a bot that is involved in a network is captured it can cause slight deviation in maintaining the false crowd situation as intended by the botmaster[13]. So a well organized intrusion detection system can trace the slightest change in the deviation between legitimate and false crowd and a botnet attack can be successfully prevented.

ACKNOWLEDGMENT

We owe our special thanks and gratitude to Mr. K. Narashimha Mallikarjunan, Assistant Professor, Department of Computer Science and Engineering, Thiagarajar College of Engineering, for his guidance and support throughout our project. We would like to thank the members of the "Parallel processing" laboratory of our college for providing information and encouragement throughout our project.

REFERENCES

[1] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of networkbased defense mechanisms countering the DOS and DDoS problems," ACM Comput. Surv., vol. 39, no. 1, 2007.

[2] M. Edman and B. Yener, "On anonymity in an electronic society: A survey of anonymous communication systems," ACM Comput. Surv., vol. 42, no. 1, 2009.

[3] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R.Kemmerer,C.Kruegel,andG.Vigna,

"Yourbotnetismybotnet: Analysisofabotnettakeover,"inProc.ACMConf.Comput.Commun. Security, 2009.

[4] Z. Li, A. Goyal, Y. Chen, and V. Paxson, "Towards situational awareness of large-scale botnet probing events," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 175–188, Mar. 2011.

[5] C. A. Shue, A. J. Kalafut, and M. Gupta, "Abnormally malicious autonomous systems and their internet connectivity," IEEE/ACM Trans. Netw., vol. 20, no. 1, pp. 220–230, Feb. 2012.

[6] M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "My botnet is bigger than yours (maybe, better than yours): Why size estimates remain challenging," in Proc. 1st Conf. Workshop Hot Topics Understanding Botnets (HotBots"07), 2007.

[7] N. Jiang, J. Cao, Y. Jin, L. E. Li, and Z.-L. Zhang, "Identifying suspicious activities through DNS failure graph analysis," in Proc. IEEE Int. Conf. Netw. Protocols, 2010, pp. 144–153. [8] S.Yadav,A.K.K.Reddy,A.L.N.Reddy,andS. Ranjan,"Detecting algorithmically generated malicious domain names," in Proc. Internet Meas. Conf., 2010, pp. 48–61.

[9] V. L. L. Thing, M. Sloman, and N. Dulay, "A survey of bots used for distributed denial of service attacks," in SEC, 2007, pp. 229–240.

[10] N.IanelliandA.Hackworth,"Botnetsasvehicleforonlinecrime,"in Proc. 18th Annu. 1st Conf., 2006.

[11] P. Wang, S. Sparks, and C. C. Zou, "An advanced hybrid peer-topeer botnet," IEEE Trans. Dependable Secure Comput., vol. 7, no. 2, pp. 113–127, Mar./Apr. 2010.

[12] M. Bailey, E. Cooke, F. Jahanian, Y. Xu, and M. Karir, "A survey of botnettechnologyanddefenses,"inProc.CybersecurityAppl.Technol. Conf. Homeland Security, 2009.

[13] Wireshark network analysis: the official Wireshark certified network analyst study guide L Chappell, G Combs – 2010

.