International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Survey on BotShark - Detection and Prevention of Peer-to-Peer Botnets by Tracking Conversation using CART

Pooja M. Pondkule[1], **B. Padmavathi**[2]

[1]P.G. Student, Department of Computer Engineering, GHRCEM, Wagholi, Pune, India

[2]Professor, Department of Computer Engineering, GHRCEM, Wagholi, Pune, India

Abstract: ***Detection of bots in peer-to-peer network is very tedious task. Their distributed nature also reveal rigidity against take-down attempts. Moreover, some bots are blatant in the communication pattern and advert the standard discovery techniques. In this system we are presenting a technique for faster detection of botnets using Classification And Regression Tree (CART).***

Keywords: Botnet, Botmaster, Data Mining, CART- Classification And Regression Tree

1. Introduction

Now a days, the Internet is an important tool used for information sharing, commerce and communication. It enables sharing of information through email and other massaging services. The affordable cost of network infrastructure allowed the internet to become a generic component of current era[9].

Botnet is a young and most harmful security threat to the internet based application. Bot is a program that runs on end-host makes operator enable to control infected system remotely. Botnet is a network of Bot infected system. Botmaster is a person who operates a botnet for remote process execution. once a bot gets installed on your system communicates with botmaster by using C&C server and waits for a command of execution[8].

Botnet life cycle consist of four steps that are given as follows:

1) Infection Stage: this is a step where your system gets compromised. Here botmaster inject a virus on to a host.
2) Rally Stage:Here, bot connects with a P2P network to compromise it.
3) Wait Stage: here bot waits for any instruction from a botmaster. Simply bot is in sleeping condition.
4) Execution Stage: here complete network is compromised and works as per botmasters instruction[1].

So there are many security threats are present in the system, to achieve a secure networking we have proposed a defence system BotShark. That will helps end user to have a secure network & early notification about the presence of bot as well as prevents a system from being a BOT.

2. Related Work

Mohammad Alauthaman, Nauman Aslam, Li Zhang, Rafe Alasem,M. A. Hossain ,"A P2P Botnet detection scheme based on decision tree and adaptive multilayer neural networks,"- in this paper they are using adaptive multilayer feedforward neural network with decision tree for P2P Botnet Detection. For feature selection CART-Classification And Regression Tree is used[1].

Saad Alsunbul, Phu Le, Jefferson Tan, Bala Srinivasan ,"A Network Defense System for Detecting and Preventing Potential Hacking Attempts,"-in this paper they present a technique in which a scanning strategy is very difficult,so hacker can't create hacking strategy easily.they are generating dynamic protocol to replace the standard protocol[2].

K.Shanthi, D.Seenivasan," Detection of botnet by analyzing network traffic flow characteristics using open source tools,"-in this paper they explore different bots and proposed a detection methodology for separating infected bots from normal system by analyzing different network data flow characteristics like packet interval time rather than payload inspection[3].

An Wang,Aziz Mohaisen, Wentao Chang ,Songqing Chen,"Delving into Internet DDoS Attacks by Botnets: Characterization and Analysis,"-to guide researchers they explore current botnet attacks lika DDoS in depth characterization of it and provide analysis in deep so can researcher can develope a new defence strategy against Botnet[4].

Dennis Andriesse, Christian Rossow, Herbert Bos," Reliable Recon in Adversarial Peer-to-Peer Botnets,"-in this paper they present an active attacks against crawler and sensor which occurs frequently and how we can easily detect botnets[5].

Dennis Andriesse, Christian Rossow, Brett Stone-Gross, Daniel Plohmann, and Herbert Bos,"Highly Resilient Peer-to-Peer Botnets Are Here: An Analysis of Gameover Zeus,"-to guide the researchers they demonstrate the Zeus-trojans and its impact on P2P network[6].

Junjie Zhang, Roberto Perdisci, Wenke Lee, Unum Sarfraz and Xiapu Luo , ″Detecting Stealthy P2P Botnets Using Statistical Traffic Fingerprints.”- this system is able to detect the stealthy P2P botnet even it uses a legal softwares. [7].

3. Proposed Work

Hacking strategies are growing so fast, to resist it we have implemented a BotShark-P2P model for botnet detection and Prevention is shown in figure.1. To improve the security level of networking we are using Botshark defence server, in which we capture a packet using JPCAP and WINPCAP, data mining algorithms are used K-means for clustering, CART for classification of similar type of packets and Naive Bayes for decision making.

1) Web Server

Conceptually, web server is a computer system which processes user request by using network protocol. In our system we are creating a E-mail web application to work a BotShark defence system to check the Bots. We are also creating a Virtual server to prevent the hacking attacks by directing a infected request to virtual server.

2) Defence Server

Defence server is created to verify the clients request. Any request to web server is allowed to pass through a defence server, for which we are proposing a new security strategy.

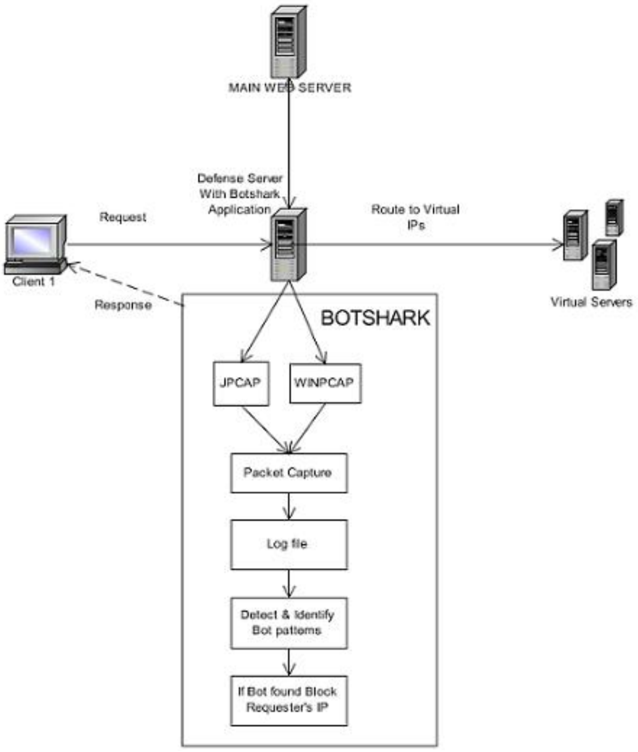

Figure 1: Architecture of the proposed system-BotShark

4. Scope of Work

Main goal of this system is to present improved method for secure networking by tracking conversation using CART.

- To present literature review of different techniques of Botnet detection.
- To present limitations of existing techniques.
- To present proposed algorithms and framework.
- To present practical analysis and performance evaluation.

5. Conclusion

In this work, we have investigated how to capture the packet to retrieve information which is useful for botnet detection can helps user to have a secure networking. To evaluate this, we proposed a new approach BotShark which extends previous approach peerShark, by using k-means for clustering, CART for classification & regression & Naive Bayes for detecting a botnet.

References

[1] Mohammad Alauthaman, Nauman Aslam, Li Zhang, Rafe Alasem,M. A. Hossain ,”A P2P Botnet detection scheme based on decision tree and adaptive multilayer neural networks,” Accepted: 17 August 2016 and published with open access at Springerlink.com

[2] Saad Alsunbul, Phu Le, Jefferson Tan, Bala Srinivasan ,”A Network Defense System for Detecting and Preventing Potential Hacking Attempts,”presented in IEEE 2016

[3] K.Shanthi, D.Seenivasan,” Detection of botnet by analyzing network traffic flow characteristics using open source tools,” IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO)2015

[4] An Wang,Aziz Mohaisen, Wentao Chang ,Songqing Chen,”Delving into Internet DDoS Attacks by Botnets: Characterization and Analysis,” 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks

[5] Dennis Andriesse, Christian Rossow, Herbert Bos,” Reliable Recon in Adversarial Peer-to-Peer Botnets,” ACM, October 28-30 2015, Tokyo, Japan

[6] D. Andriesse, C. Rossow, B. Stone-Gross, D. Plohmann, and H. Bos, “Highly resilient peer-to-peer botnets are here: An analysis of gameover zeus,” in Malicious and Unwanted Software:” The Americas”(MALWARE), 2013 *8th International Conference on. IEEE*, 2013, pp. 116–123.

[7] J. Zhang, R. Perdisci, W. Lee, U. Sarfraz, and X. Luo, “Detecting stealthy p2p botnets using statistical traffic fingerprints,” in Dependable Systems & Networks (DSN), 2011 *IEEE/IFIP 41st International Conference on. IEEE*, 2011, pp. 121–132.

[8] C. Rossow, D. Andriesse, T. Werner, B. Stone-Gross, D. Plohmann, C. J. Dietrich, and H. Bos, “Sok: P2PWNED-modeling and evaluating the resilience of peer-to-peer botnets,” in Security and Privacy (SP), 2013 *IEEE Symposium on. IEEE*, 2013, pp. 97–111.

[9] J. Li, S. Zhang, Y. Lu, and J. Yan, “Real-time p2p traffic identification,” in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE. IEEE*, 2008, pp. 1–5.

[10] M. Iliofotou, H.-c. Kim, M. Faloutsos, M. Mitzenmacher, P. Pappu, and G. Varghese, “Graph-based p2p traffic classification at the internet

backbone," in *INFOCOM Workshops 2009, IEEE. IEEE*, 2009, pp. 1–6.

[11] D. Dittrich and S. Dietrich, "P2p as botnet command and control: adeeper insight," in Malicious and Unwanted Software, 2008. MALWARE 2008. *3rd International Conference on. IEEE*, 2008, pp. 41–48.