International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 4, Special Issue 3 (March '2018)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

DDOS BOTNET DETECTION AND IDENTIFICATION CHALLENGES AND STRATEGIES IN PEER TO PEER SYSTEMS

Prema A,
Assistant Professor,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

Praveen S L,
Student,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

Vamsi Krishna AV,
Student,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

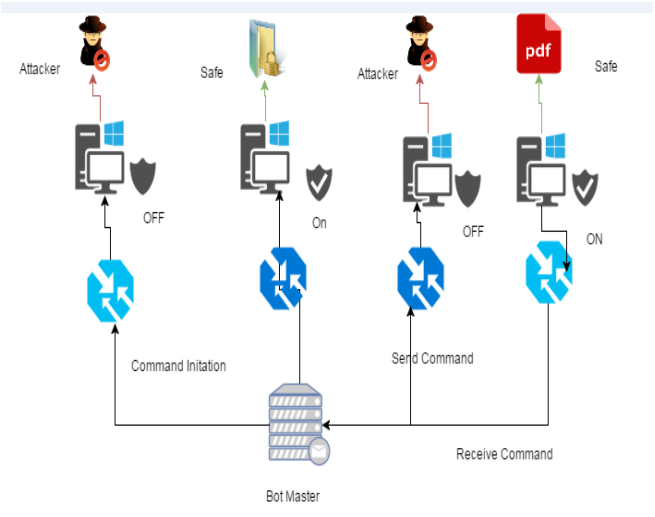
Dinesh Krishnan J,
Student,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

Abstract: Botnets are the foremost mundane conveyance of cyber-malefactor activity. They're utilized for spamming, phishing, denial-of-accommodation attacks, brute-force cracking, purloining non-public data, and cyber. A botnet (also referred to as a zombie army) may be a range of network computers that, though their homeowners are unaware of it, are got wind of to forward transmissions (including spam or viruses) to alternative computers on the web. During this paper, we have a tendency to propose a two-stage approach for botnet detection. The primary stage detects and collects network anomalies that are related to the presence of a botnet whereas the second stage identifies the bots by analyzing these anomalies. Our approach exploits the subsequent 2 observations: (1) bot masters or attack targets are easier to find as a result of the impact with several alternative nodes, and (2) the activities of infected machines are a lot of correlative with one another than those of traditional machines.

Keywords: anomalies, tendency, purloining

I.INTRODUCTION

CYBER-SECURITY ranks among the biggest challenges of modern times. Whether we are talking about phishing, website sabotages, or even of terrorist attacks, protecting our digital lives is an issue of paramount importance. Networks, and especially the Internet, became the natural attackers' habitat to hide a broad variety of threats. For instance, a dangerous attack to a powerful target site (e.g., a big e-commerce portal) is often launched through a series of apparently innocuous attacks to some powerless, but most vulnerable, sites (e.g., some personal computers). One of the most popular threats is the Denial-of-Service (DoS) attack, which can be broadly categorized as a volumetric attack, where the target destination is overwhelmed by a huge number of requests, eventually leading to the impossibility of serving any of the users. In particular, with a Distributed DoS (DDoS) attack, such a huge number of requests is produced in parallel by a set of robots (the botnet). According to one of the classical DDoS Nrepresentations, a relatively large ensemble of machines (the bots or zombie "army"), acts cooperatively under the supervision of one or more coordinators (the botmasters). The bots may be either themselves malicious users acting consciously, or they may be legitimate users that have been preliminarily infected, (e.g., by worms and/or Trojans). The existence itself of an anomalous request rate is essentially uncovered, and, hence, its detection is not a big deal. The main challenge is instead ascertaining whether the anomaly is caused by a DDoS attack, and, if so, performing a correct/early identification of the botnet hidden in the network. These operations are crucial to achieving successful DDoS mitigation, since discriminating legitimate from malicious users would allow the destination to ban the latter, without denying the service to the former. Providing inference solutions to botnet discovery and identification is the main subject of this work.



II.EXISTING SYSTEM

We need linger clustering-based analysis behave to catch a glimpse of hosts that are virtually likely one after the other P2P applications. The concern does not accept any sack layer secondhand by which gave a pink slip be no ifs ands or buts about it violated by P2P applications. It is mainly merit to the article that the intercourse profile of a bot-compromised mistress of the household might be plenarily untrue by the precise P2P academic work one after the other on it simultaneously. For instance, in our experiments, when a mistress of the household is continually a Waledac and a Bit Torrent application simultaneously.

TECHNIQUE DEFINITION:

A bot-compromised host might be completely distorted by the legitimate P2P application running on it simultaneously. Servers are that they represent a single point of failure.

DRAWBACK

The fundamental disadvantage of centralized C&C. Servers are that they represent a single point of failure.

PROPOSED CONCEPT

Here we focus various botnet types which performing direct type and rule over botmaster, transpire well-determined interval

This paper offers a detailed dissection of the botnet's scanning behavior, including general methods to correlate, visualize, and extrapolate botnet behavior across the global Internet.

PROPOSED TECHNIQUE

Course Grained BotNet Detection which is used to detect the file in well specified manner and that can process all the file in that network.

TECHNIQUE DEFINITION:

P2P botnets before they are detected in contrast to our approach can detect and profile various P2P applications. Identifying a specific P2P application.

ADVANTAGE

We also identify the performance bottleneck of our system and optimize its scalability.

We presented a novel botnet detection system that is able to identify stealthy botnets, whose malicious activities may not be observable.

FUTURE CONCEPT

To summarize, although our system greatly enhances and complements the capabilities of existing P2P botnet detection systems, it is not perfect. We should definitely strive to develop more robust defence techniques, where the aforementioned discussion outlines the potential improvements in our system. We also identify the IP address of the bot attacker.

FUTURE TECHNIQUE: -

Non Legimative Detection which will do all the process to detect file in the network this is enhanced as future technique.

TECHNIQUE DEFINITION:

Botnet developers are constantly improving their development in order to produce more and more stealthy malware for all kinds of attacks to make the profit.

EXTRAVAGANCE:

While sundry approaches have been studied or utilized for botnet attacks, the jeopardy of exploiting widely used browser extensions and their automatic browser extension update.

III.CONCLUSION

Previous detection approaches have some weaknesses such as less accuracy, high FPRs, unable to detect stealthy botnets, advanced botnets using FFSNs and botnets using rootkits. All these problems are solved by various recent approaches described here. Table 2 provides a summarization of all the techniques discussed along with their advantages and limitations. These techniques are able to detect P2P botnets with very high detection accuracy and very fewer FPRs. But none of the techniques discussed here is solely able to address all the problems of P2P botnet detection. However, we can develop techniques by combining two or more techniques, which will exclusively address all the detection problems of P2P botnets.

IV.REFERENCES

[1]. W. Stallings, Cryptography and Network Security: Principles and Practice, 6th ed., Pearson, 2013.

[2]. N. Hoque, D. Bhattacharyya, and J. Kalita, "Botnet in DDoS attacks: trends and challenges," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2242–2270, fourth quarter 2015.

[3]. L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," in Proc. DARPA Information Survivability Conference and Exposition, Washington, DC, USA, Apr. 2003, pp. 303–314.

[4]. J. Yuan and K. Mills, "Monitoring the macroscopic effect of DDoS flooding attacks," IEEE Trans. Depend. Secure Comput., vol. 2, no. 4, pp. 324–335, Oct. 2005.

[5]. L. Li, J. Zhou, and N. Xiao, "DDoS attack detection algorithms based on entropy computing," in Proc. ICICS 2007, Zhengzhou, China, Dec. 2007, pp. 452–466.

[6]. Y. Xiang, K. Li, and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics," IEEE Trans. Inf. Forensics and Security, vol. 6, no. 2, pp. 426–437, Jun. 2011.

[7]. J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, "On a mathematical model for low-rate shrew DDoS," IEEE Trans. Inf. Forensics and Security, vol. 9, no. 7, pp. 1069–1083, Jul. 2014.
[8]. "Layer 7 DDoS." HTTP://blog.sucuri.net/2014/02/layer-7-DDoS-blocking HTTP-flood-attacks.html.
[9]. "Taxonomy of DDoS attacks." http://www.riorey.com/types-of-ddosattacks/#attack-15.
[10]. "Global DDoS threat landscape." https://www.incapsula.com/blog/ddosglobal-threat-landscape-report-q2-2015.html.
[11]. S. Ferretti and V. Ghini, "Mitigation of random query string DoS via gossip," Commun. in Comput. and Inf. Sci., vol. 285, pp. 124–134, 2012.
[12]. S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of Byzantine attacks," IEEE Trans. Signal Process., vol. 57, no. 1, pp. 16–29, Jan. 2009.
[13]. S. Marano, V. Matta, and P. Willett, "Distributed detection with censoring sensors under physical layer secrecy," IEEE Trans. Signal Process., vol. 57, no. 5, pp. 1976–1986, May 2009.
[14]. M. Barni and B. Tondi, "The source identification game: an information theoretic perspective," IEEE Trans. Inf. Forensics and Security, vol. 8, no. 3, pp. 450–463, Mar. 2013.
[15]. B. Kailkhura, S. Brahma, B. Dulek, Y. S Han, and P. Varshney, "Distributed detection in tree networks: Byzantines and mitigation techniques," IEEE Trans. Inf. Forensics and Security, vol. 10, no. 7, pp. 1499–1512, Jul. 2015.
[16]. M. Mardani, G. Mateos, and G. B. Giannakis, "Dynamic anomalography: tracking network anomalies via sparsity and low rank," IEEE J. Sel. Topics Signal Process., vol. 7, no. 1, pp. 50–66, Feb. 2013.
[17]. M. Mardani, G. Mateos, and G. B. Giannakis, "Recovery of low-rank plus compressed sparse matrices with application to unveiling traffic anomalies," IEEE Trans. Inf. Theory, vol. 59, no. 8, pp. 5186–5205, Aug. 2013.
[18]. M. Mardani and G. B. Giannakis, "Estimating traffic and anomaly maps via network tomography," IEEE/ACM Trans. Networking, DOI: 10.1109/TNET.2015.2417809, date of publication, Apr. 2015.

