ISSN No:-2456-2165

Survey on Software Defined Network based Botnet Attacks

Rajni Samta[1], Pooja Rani[2]
[1, 2]Department of Computer Science, Himachal Pradesh University, Shimla, India

Abstract:- Software Defined Network has been a solution to those problems which have emerged with the advancement of social interconnection through internet, cloud computing and internet of things. Along with the speed and efficiency of any network, there are certain other parameters which are of great importance for an organization. These organizations are demanding more flexible networks which are dynamic enough to change or mould the network according to their needs. Software Defined Network breaks the barriers of traditional way of networking, where as it is cost efficient as it simplifies hardware and software management, any change in the software defined networks are easily adopted. This paper has discussed about a major security threat that has emerged in past few years called botnets and also has discussed related work regarding Software Defined Network based botnets.

Keywords:- *Software Defined Networks, Botnets, zombie Networks, Command and Control(C&C), (P2P) Peer to peer Botnet, Internet Relay Chat (IRC) Botnet, HTTP Botnet.*

I. INTRODUCTION

BOTNET: Malicious software or malware can harm our computers in variety of ways, in sometimes the affects are not known until it's too late and in worse scenario our computers can become one of many infected malware creating botnet. Botnet is a term that is short for robot and network [1]. Cyber Criminals use special malware usually a Trogon horse to breach the security of several computers and take control of each computer and organize these infected machines into a network of bots. Which is then used as a tool that a cyber criminal can remotely manage, the infected system may completely act normal with no warning signs [2, 3, and 4]. A bot can be a MAC, Personal Computer or even a Smartphone. Often time cyber criminal seek to involve and control thousands, ten thousands and even millions of computers, so that they can be a master of large Zombie network. These Botnets are capable of delivering several types of cyber crimes such as DDoS attacks, Spreading malware, online fraud and phishing campaign. Figure 1 [5], shows the illustration of Botnet attack.

TYPES OF BOTNETS: The three basic types of botnet are Command and Control (C&C) technologies: IRC (Internet Relay Chat) based, HTTP (or Web) based and P2P (Peer-to-peer) based.

- COMMAND AND CONTROL (C&C): As we know various compromised computers compose a network that is used by a Botmaster for malicious purpose. Hence there is a need of some kind of communication between Bots and Botmaster, which is command and control (C&C) [6]. For example, A Bot reports its status to Botmaster or a Bot could receive instructions for spam, phishing or DDoS etc. whereas a Bot can be directed to some site to download a malware. Therefore without (C&C) a Botnet is not a network. Hence (C&C) is very important aspect of Botnet, without it a Botmaster cannot utilize the individual computational powers of the infected machines fully [7].
- (P2P) BOTNET: A (P2P) network sometimes refers to as a Peer to Peer network. It is more complicated Botnet because each infected machine works as its own (C&C) and it does not contain any central point of command and central point of failure which is very hard to take down as an investigator [8]. Commands are propagated across the network and it might take a long time for single command to go through entire network hence it increases latency [9]. So, different machines may act differently by getting a specific role to perform, such as some might become proxy machines to hide the actual Botmaster, some might act as spam instructor nodes where as some might become the critical components of the Bot network so that the investigators will not be able to crack the network pattern [10].
- (IRC) BOTNET: Internet Relay Chat is the most commonly talked about botnet types. This type of botnet attack uses TCP protocol and these IRC Bots can be customized using different scripting languages [10, 11]. These were initially created to promote automated commands and for the automation of the channel, but this feature of IRC were turned into a malicious automated attack [12].
- HTTP BOTNET: Hypertext transfer protocol is a commonly used network protocol and thus http botnet is an easily implemented botnet than P2P, as it is also a web based botnet, and all the commands are sent through http protocol. Because of http header all malicious code is masked under http protocol packets[12, 13].

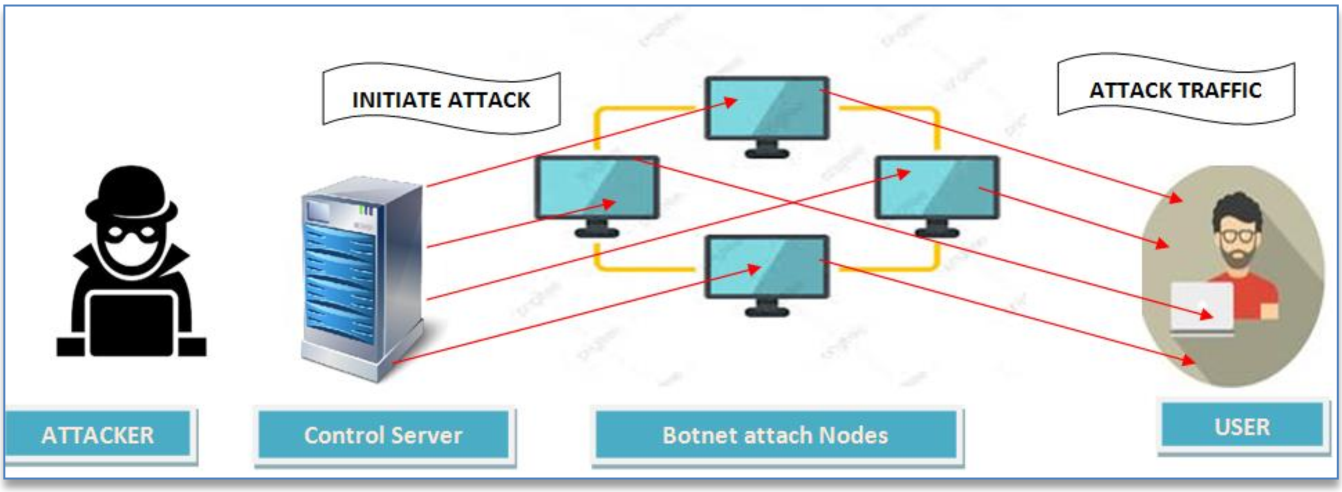

Fig 1:- Illustration of Botnet Attack [5].

II. REVIEW OF LITERATURE

Silva, S. S. C. et al. [1] one of the serious threats that are formed by various compromised machines also known as Botnets have been indulging in various scams that are sometimes minor or sometimes large scale activities. Every year some illegal Botnet activity keeps this treat a fresh topic now days for research purpose and has increased number of publications for this topic in past few years. Through this paper Silva, S. S. C. and other authors have tried to discuss various problems regarding botnet and has discussed some existing studies and some recent work concluding some suggestions and solutions.

Zhu, Z. et al. [2] keeping in mind the number of infected malicious machines the botnet has been a major threat, the numbers are around 40-45 % of the total computers systems connected to the internet. This paper has tried to classify the problems regarding the Botnet, the main classifications they have proposed are: Understanding the Botnets, giving the brief idea about what botnets are. Second classification is detecting and tracking botnets and lastly defending the Botnets. This paper is giving a clear view of various future topics for research in botnets.

Feily, M. et al. [3] have discussed how botnets can be a major threat to the network society as it is capable of providing a platform for various dangerous threats like distributed denial of service attacks, malware dissemination, and phishing and click fraud. This survey has given a clear classification of botnet detection techniques. The classes of Botnet Detection technique that has been discussed are Mining based, DNS Based, Anomaly based and Signature based.

Chen, J. Cheng, X. et al. [4] in this paper, they have discussed the computation complexities of botnet. Moreover they have also proposed lightweight real time botnet detection technique.

III. CONCLUSION

Network data security should be a high priority when considering a network setup due to the growing threat of hackers trying to infect as many computers possible. For corporations, security is important to prevent industry sabotage and espionage. Imagine what can happen if there is a network integrity breach at a bank, stock exchange, or other financial database. Likewise DDoS based botnet attacks are major threat to internet as they are capable of doing various possible damages to a network, as it can invade any computer connected to network. Social engineering can be a key factor in propagation of this malicious software and turning the computer as a bot. According to various reports and survey, one out of four computers has been compromised major examples in real world in past years are ZEUS, CUTWAIL, BREDOLAB, WALEDAC. Such attacks and bots must be detected and should be mitigated. The software defined network being a flexible and it easily adopts any changes made to the network is a good option for network security. As software defined networks have their own ways of detecting and also mitigating such kinds of security threats to the networks.

REFERENCES

[1]. Silva, S. S. C., Silva, R. M. P., Pinto, R. C. G., & Salles, R. M. (2013). Botnets: A survey. Computer Networks, 57(2), 378–403. doi:10.1016/j.comnet.2012.07.021.

[2]. Zhu, Z., Lu, G., Chen, Y., Fu, Z. J., Roberts, P., & Han, K. (2008). Botnet Research Survey. 2008 32nd Annual IEEE International Computer Software and Applications Conference. doi:10.1109/compsac.2008.205

[3]. Feily, M., Shahrestani, A., & Ramadass, S. (2009). A Survey of Botnet and Botnet Detection. 2009 Third International Conference on Emerging Security Information, Systems and Technologies. doi:10.1109/securware.2009.48.

[4]. Chen, J., Cheng, X., Du, R., Hu, L., & Wang, C. (2017). BotGuard: Lightweight real-time botnet detection in software defined networks. Wuhan University Journal of Natural Sciences, 22(2), 103–113. doi:10.1007/s11859-017-1223-8.

[5]. Su, S.-C., Chen, Y.-R., Tsai, S.-C., & Lin, Y.-B. (2018). Detecting P2P Botnet in Software Defined Networks. Security and Communication Networks, 2018, 1–13. doi:10.1155/2018/4723862.

[6]. E. Cooke, F. Jahanian, D. McPherson, The zombie roundup:understanding, detecting, and disrupting botnets, in: Proceedingsof the Steps to Reducing Unwanted Traffic on the Internet on Stepsto Reducing Unwanted Traffic on the Internet Workshop, USENIXAssociation, Berkeley, CA, USA, 2005, p. 6.

[7]. H. Choi, H. Lee, H. Kim, BotGAD: detecting botnets by capturinggroup activities in network traffic, in: Proceedings of the FourthInternational ICST Conference on COMmunication System softWAreand middlewaRE, COMSWARE ’09, ACM, New York, NY, USA, 2009,pp. 21–28.

[8]. J.M. Ceron, L.Z. Granville, L.M.R. Tarouco, Uma arquitetura baseadaem assinaturas para mitigaßc~ao de botnets, in: X Simp´osioBrasileiro em Seguranßca da Informaßc~ao e de SistemasComputacionais (SBSeg), pp. 105–118.

[9]. B. AsSadhan, J. Moura, D. Lapsley, C. Jones, W. Strayer, Detectingbotnets using command and control traffic, in: Eighth IEEEInternational Symposium on Network Computing andApplications, 2009. NCA, 2009, pp. 156–162.

[10]. M. Fossi, G.Y. Egan, K. Haley, E. Johnson, T. Mack, T. Adams, J.Blackbird, M.K. Low, D. Mazurek, D. McKinney, P. Wood, SymantecInternet Security Threat Report – Trends for 2010, Technical ReportVolume 16, Symantec, 2011.

[11]. C. Li, W. Jiang, X. Zou, Botnet: survey and case study, in: FourthInternational Conference on Innovative Computing, Informationand Control (ICICIC), 2009, pp. 1184–1187.

[12]. D. Plohmann, E. Gerhards-Padilla, F. Leder, Botnets: Detection,Measurement, Disinfection & Defence, Technical Report, TheEuropean Network and Information Security Agency (ENISA), 2011

[13]. M.A Rajab, J. Zarfoss, F. Monrose, A. Terzis, A multifaceted approachto understanding the botnet phenomenon, in: Proceedings of the6th ACM SIGCOMM Conference on Internet Measurement, IMC’06,ACM, New York, NY, USA, 2006, pp. 41–52.