THINK INDIA JOURNAL
ISSN: 0971-1260
Vol-22-Issue-3-July-2019

A Survey on Botnet Attack, Its Detection and Defense Mechanismin Software Defined Networking

Mehak[1], Upinder Kaur[2], Swati[3]
School of Computer Science & Engineering
Lovely Professional University, Phagwara, Punjab, India
mehakkatnoria93@gmail.com[1], upinderkaur45@gmail.com[2], rampalswati@gmail.com[3]

***Abstract*—**Among different malware categories, botnets are developing as one of the most valid danger for digital security as they give the stage to many criminal operations, for example, Administrative assaults against basic targets, malware spread and phishing attack. The characterizing norm for botnets is the utilization of order and control channels via which they can be refreshed and co-ordinated. Today, discovery of a botnet discovery has been an essential subject as botnet possess a digital danger and its counter measure. This paper is an overview of botnet and its detection, along with its defense. The study explains botnet's crux and examines botnet location methods. This assessment characterizes botnet reputation techniques into four sections: signature-based, irregularity-based, DNS-based, and mining-base. This paper presents the audit of Software Defined Networking (SDN), security and possible danger, particularly against botnet. SDN framework works in a centralized manner, control, and activity with isolated control and information plane. By means of this framework, bot-master can implant and unfold their contamination through SDN control plan as an unauthenticated PC. This issue is regarded as CIA Integrity, set of three (Confidentiality, Integrity, and Availability), that is utilized for evaluation of security performance of SDN.

Keywords:*Botnet, Integrity, Botnet Detection, Cyber-security, Software Define Networking;*

1. Introduction

As per clarification in [1, 2], malicious botnet is defined as "a system of compromised computer systems, called *Bots* which is under the remote control of an administrator called *Botmaster*."The expression "*Bot*" is derived from "Robot" and like robots, bots are intended to play out some predefined capacities in computerized way. As such, the bots are programs that gives the control to the botmaster who will have the ultimate control all the activities of compromised system. Botnets represent a noteworthy and developing danger against digital security as they give a circulated stage to numerous digital violations, for example, Distributed Denial of Service (DDoS) assaults against basic targets, malware spread, phishing, and click fraud [3,4]. Researchers have suggested many botnet identification methods to counter cyber-security botnet risk.

SDN[5-7] as another innovation in organized improvement assumes a job is brought together for setup, control, and activity arrangements. It can engage architectures, cost productivity, and offer the chance to new system application or work by updating programming framework. SDN has not been very much perceived by the security network yet [8]. On the other side,SDN can possibly be assaulted alongside mechanical development.Botnet assault is one sort of assault that turned into the fundamental risk to the conventional system that gets an opportunity to turn into a risky danger in SDN. The motivation behind why botnet is picked as one of different assault is due to its effect on

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

disturbance for trustworthiness.Integrity is one of the CIA (*Confidentiality, Integrity, Availability*) Triad part that utilized as security parameter to organize security. Integrity in CIA is a condition where data is kept exact and predictable except if approve changes are made.

This survey classifies botnet detection approaches into four classes: signature-based, irregularity based, DNS-based, and mining-based. Furthermore, the paper is organized as follows: in Section 2, SDN potential attack to each architecture that is vulnerable to be attacked is explained. Section 3 describes about botnet which includes overview and architecture. In this segment, botnet qualities and botnet life-cycle are disclosed to give better comprehension of botnet innovation. Segment 4 talks about botnet detection and tracking. In this area, four classes of botnet location approaches including mark based, inconsistency based, DNS-based, and mining-based are examined separately. In Section 5, SDN defense against Botnet is discussed. In Section 6, the survey has been concluded and future scope has been discussed.

2. Features of SDN

SDN provides advantages with four characteristics divided as follows:

i. *Dynamic Flow Control:* SDN can powerfully control information stream on the system. With this element, SDN information stream can be controlled productively. Noxious system bundles stream can be isolated from approved streams without setting up new center boxes and it very well, may be finished with arrange gadget.Programmable BYOD Security(PBS) [9] is a case of this component, it awards to administrator for building up and install virtual SDN.

ii. *Integrate Extensive Visibility Monitoring:* Directs and deal with the general system to obtain all status of system and information flow.NetSecVisor [10] can use security gadgets and influence SDN ability to be virtualized.

iii. *Programmability network*: System ply on SDN control plane is modified Application Programming Interfaces (APIs) [11]. It makesnetwork security simpler bythesetting up of the security application program. One of this elementinstancesis FRESCO [12].

iv. *Easy Data Package*: SDN separates control and information plane. It makes SDN information planemore straightforward and an open door for including information plane expansion for security work. OFX (Open Flow Extension Framework) [13] is one of its features,OFX can empower SDN security application with existing Open Flow.

2.1 Potential Attack onSDN:

On the basis of [14], there are a few possible security issues in the SDN which are assembled into couple of points as shown in Figure 1 below and discussed in the following points:

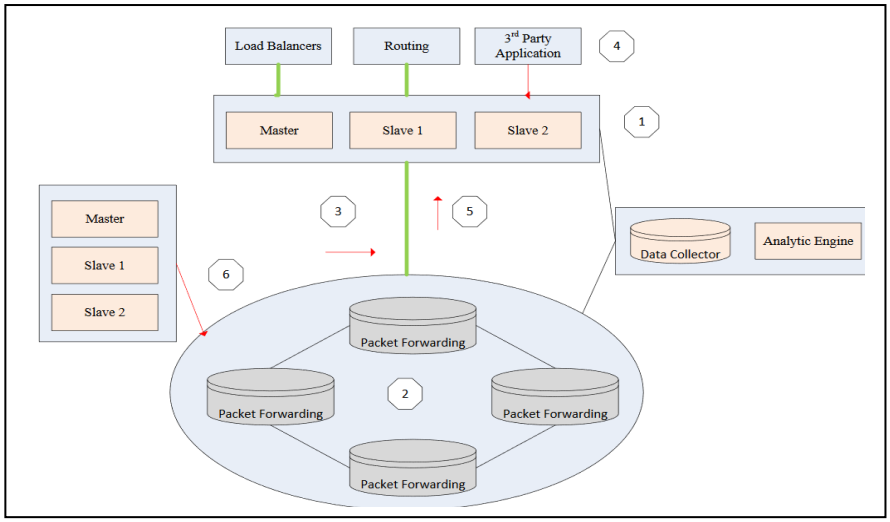
i. *Unauthorized Access:*Access refers to the control of access. There are some possibilities for attackers disguised as controllers or 3rdparty applications. An attacker could gain privileges to arrange various settings and control multiple activities on the system.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

ii. *Data Leakage:*SDN packet handling has a few probable actions like forwarding, drop and sendingcontroller the packets [14]. Through this system, it is possible for an attacker to analyze the behavior for the packet stated, by analyzing the time of the arrival of the packet, as packet forwarding to the controller is longer than other packets.

iii. *Data Modification:* The attacker gets an opportunity to adjust information at whatever point they can commandeer controller for the whole framework. If such situation arises, an attacker may modify the injection flow rules in network devices to allow an attacker advantage to control the packet.

iv. *Denial of Services*: Inseparate control and data plane are the main weakness of SDN. This is because the path of inthecommunication between the controller and the network device attacker might spam and overflow,making



services unavailable on the network[15].

Fig.1: Potential Attack on SDN

v. *Configuration Issues:*As the programmable device, SDN has safety vulnerabilities since it may be defenseless particularly for information or control correspondence.

3. About Botnet

Botnets are a huge risk for the web environments and processing of resources. Harmful botnets are utilized for criminal operations, for example, Distributed Denial of Service (DDoS) attacks, transmittingmalicious mail and phishing messages to the victim's computer, unlawfully send illegal media, stealing information (also called *information theft*) and many more [16]. Botnet is unique in relation to different kinds of attacks in the presence of C&C. Itsends requests from botmaster to the bots.Bots consistently search for a target. When bot discover the target,they're going to send the target's information to the botmaster [17].Also, each bot is not physically controlled by the botmaster, and might be situated in different parts of the planet. Difference in various time zones, dialects, and

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

rules and regulationsit is hard to follow pernicious botnet exercises over globe [2]. This feature makes botnet a serious danger and creates a major threat to cyber security.

3.1 Botnet's Lifecycle

It is possible to create and sustain a standard botnet in five steps which involves: *basic infection, secondary intrusion, link, mischievous command and management, updating and maintenance*. The life-circleof Botnet is demonstrated in Figure 2 below:

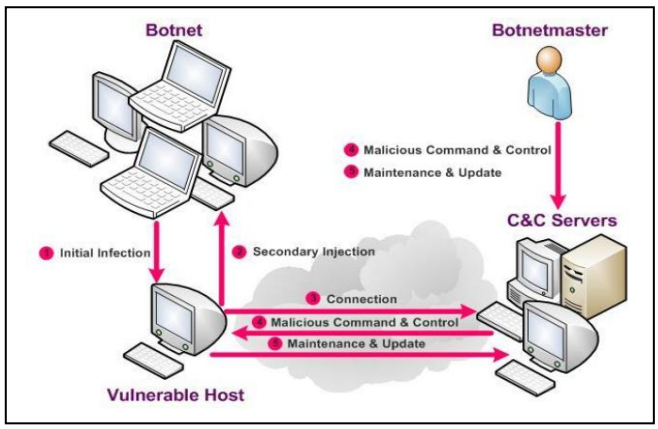


Fig. 2: Botnet Life-cycle

The attacker finds a target subnet for a known vulnerability during the *initial infection process* and infects victim machines via various methods of exploitation. After the initial infection, the affected hosts run a script called*shell code* in the secondary injection process.Shell code collects the image from the specific location of the actual binary bot through FTP, HTTP, or P2P. The binary bot on the target machine is installed itself. The victim computer transforms to a "Zombie" once the bot software is downloaded and runs the malignant code.When the zombie reboots, the bot application starts accordingly [2, 18].

The bot software creates a stream of command and control (C&C) in the *communication phase*, and links the zombie computer systemand server of command and control (C&C). Once the C&C channel is established, the zombie is now part of the botnet.The real tasks of command and control of the botnet will be started after the link process. The botmaster makes use of the C&C network to disperse his bot army's orders. Bot programs are receiving and executing botmaster commands. The C&C channel assists the botmaster in tracking the activityof large numbers of bots remotely to perform various illegal tasks[18].

Last stage is keeping up bots exuberant and refreshed. For a few reasons, bot controllers can replace their botnets.For example, they might need to refresh the bot parallel to sidestep identification methods, or they will anticipate to add new usefulness to their bot armed force. Besides, once in a while the refreshed two-foldploy the bots to an alternate C&C server. This procedure is defined as server movement and are highly helpful in preserving their botnet alive [2,19]. Botmasters try to preserve their botnets undetectable

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

and compact by utilizing Dynamic DNS (DDNS) [20] that encourages updates and modifications in server areas.

3.2 Architecture of Botnet

To hide the C&C architecture, Botmaster controls its C&C (Command and Control) to engage in a roundabout way with its bot. There are three topologies listed, as follows, on the Botnet attack in Figure 3, 3 topologies on Botnet:

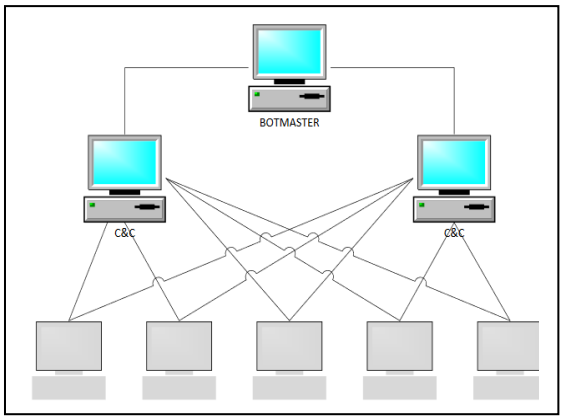


Fig.3:Condensed(centralized) C&C Server

1. *Condensed/Centralized C&C Server:*It is the most seasoned kind of botnet structure, which give moderate idleness, obscure, and ongoing correspondence to botmaster with a main issue of conveying a message from botmaster to interact with their bot [17]. This topology's drawback is that if C&C server is tracked, all botnet systems will be of no use. Couple of instances are AgoBot, RBot and SDBot.

1.1 *Botnet IRC:*Figure 4 below depicts the scheme of IRC Botnet attack, IRC is a textual content message sent at the internet [21,22]. The protocol is based totally on the client-server model, which is used on a computer with distributed network. The upsides of utilizing IRC convention on botnet are:

a. Low latency on communication side.
b. Communication in real time is concealed.
c. Have the working ability in groups and in pairs.
d. Easy installation.
e. Flexible communication

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

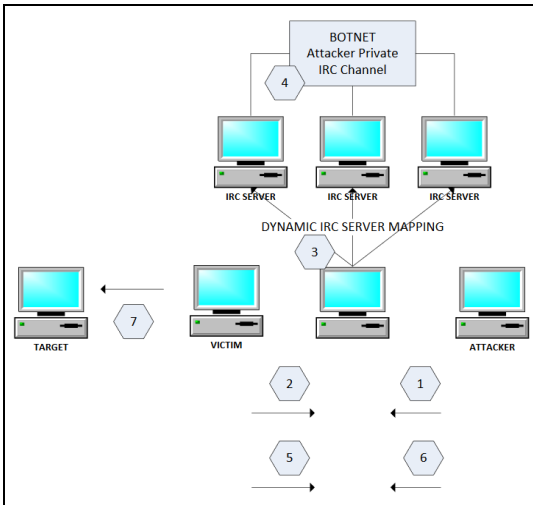


Fig. 4: Botnet IRC

In this manner, the IRC convention is a well-known convention utilized in botnet communication.

1.2 *Botnet HTTP:* The attacker began using HTTP Botnet, making it hard to find the botnet. This is on the grounds that the botnet utilizes the HTTP convention to hide the presence of its bot in web traffic, making it simple for botnets to sidestep the firewall utilizing a port-based sifting system and maintain a strategic distance from IDS identification. The firewall can limit incoming visitors and outbound visitors to unnecessary ports that entails IRC ports under normal circumstances. HTTP botnet's few examples are Rustock, Bobax, and ClickBot [17]. Below figure, Figure 5, shows the structure of HTTP botnet as:

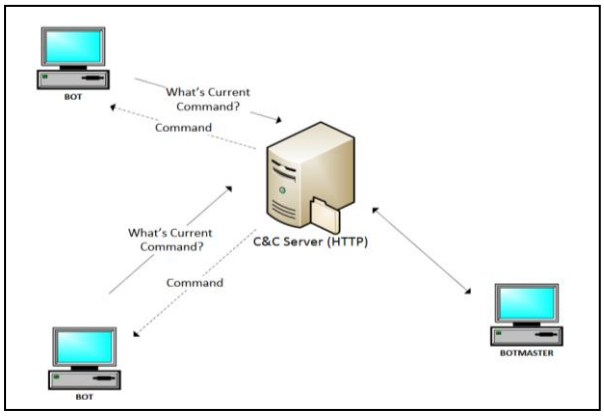


Fig.5: HTTP Botnet

2 *Hybrid:*It is the higher version of P2P [23],bot on this sort is classified as:

a. *Servant Bots*: The bot functions as a consumer and server with static IP addresses that are routable and easily attainable from the internet.

b. *Client Bots:*Bots act as customers because incoming connections are not accepted [28]. The remaining bots are in this class as follows:

i. Bots' dynamic IP addressing properties.

ii. Fixed route IP address of bot.

iii. Bots working behind a firewall, that can't connect to the global internet.

The following figure, Figure 6, shows the Hybrid Botnet.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

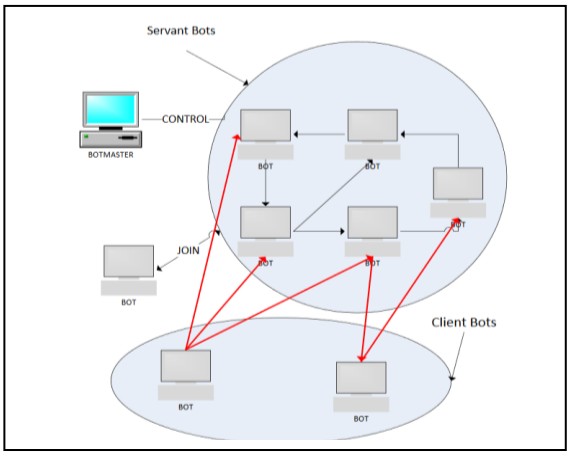


Fig. 6:Hybrid Botnet

3 *Decentralized or Peer to Peer C&C Server:*Attackers use the system of peer-to-peer interaction as an example of C&C, which thus gives a bit of leeway in keeping away from organize failures. Bot has a limited size in this topology and each bot is connected to a neighbor to receives a botmaster command on a regular basis. In this topology, Botmaster only needs to connect to one bot. Figure 7 belowindicates the lack of a centralized point of interaction, each bot interacts with other bots.

At the other hand, the bot also participates in the transmission of data as a client and server. The newly affected bot must learn the other botnet linked to it. If the bot is in offline mode, under the botmaster command, other bots can continue operations. P2P botnet seeks to eradicate the presenceof failure in a hierarchical system or significant vulnerability.

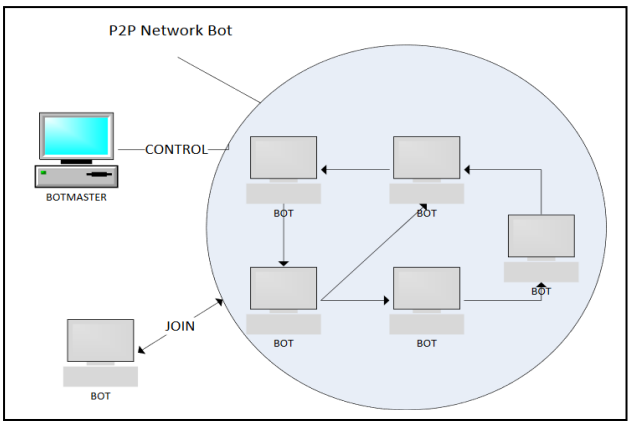


Fig. 7: Peer to Peer C&C Server

4 Botnet Detection

There are two main approaches to detecting and tracking the botnet [24]. One solution is based on honeynets being set up. For example, solutions in [24] were initial solutions based on honeynet.Honeynets are, broadly speaking beneficial for knowledge botnet era and functions, but they may or may notexpose bot infection. The alternative technique to botnet

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

detection is primarily based on passive network traffic tracking and analysis.Botnet identification techniques are useful for identifying the presence of botnets based on passive traffic monitoring. The techniques are categorized as *Signature-Based*, *Anomaly-Based*, *DNS-based*, and *Mining-Based* techniques that are respectively defined and explained in this section.

A. *Signature-BasedDetection*: It is helpful for botnet detection to know the needful signatures and nature of botnets which already exists. An open source intrusion detection system (IDS), for example, Snort, which monitors network traffic to detect intrusion signs. Like maximum IDS systems, Snort is set up to log traffic witha collection of laws that are deemed suspect [25].

B. *Anomaly-based Detection:* It endeavors to recognize botnets dependent on a few system traffic inconsistencies, for example, high system idleness, high traffic volumes, traffic on rare ports, and surprising framework conduct that could demonstrate nearness of malignant bots in the system [1]. Though anomaly detection techniques resolves unidentified botnets question detection, it may include an IRC network capable of being a botnet but not yet used for attacks. Binkley and Singh [26] have proposed a compelling algorithm joining TCP-based irregular identification of IRC tokenization and measurements of IRC messages to create a framework that can be unmistakably recognize customer botnets. This phenomenon may expose bot servers as well.

   Detecting novel botnets with high accuracy and low false positivity is a challenge. Cid-Fuentes, *et al*. [27] address this problem in a scalable and decentralized context. Their framework creates a complete characterization of legitimate hosts ' behavior that can be used to discover botnet traffic previously unseen. Their framework also adapts dynamically to changes in network traffic and is able to detect new botnets without any assumption about their architecture or protocols.

C. *DNS-based Detection*: They are established on specific botnet-generated DNS data. DNS-based detection techniques are similar to anomaly detection techniques as DNS traffic uses similar anomaly detection algorithms. DNS queries are performed to locate the respective C&C server typically hosted by a DDNS provider in order to access the C&C server bots. Thus, botnet DNS traffic can be detected by DNS monitoring and DNS traffic anomalies can be detected [28].

D. *Mining-based Detection*: The powerful method for botnet identification is to recognize botnet C&C traffic. Be that as it may, botnet C&C traffic is hard to distinguish. Indeed, botnets use typical conventions for C&C traffic, the traffic is like ordinary traffic. Additionally, the C&C traffic isn't huge and do not create high system inertness [29].Many data mining techniques can be used effectively to detect botnet C&C traffic, including machine learning, classification and

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

clustering.Botminer[27] is the latest approach to botnet C&C traffic detection using data mining criteria. Botminer is Botsniffer's improvement. This clusters similar interaction and traffic that is malicious. It then conducts cross-cluster analysis to classify hosts that haveanalogous patterns of communication and similar patterns of pernicious activity [30]. One of an ingenious method for botnet identification is Botminer which is self-reliant protocol.

4.1 Comparison of Different Botnet Detection Methods

There are many available techniques to reveal and abandon the botnet, but to detect the botnet, none of the mentioned techniques is 100% definite. Every method is constructed with the usage of various protocols and consequences in different ways. Since all below mentioned methods have certain strengths and disadvantages, the comparison of different techniques for botnet detection is shown in Table 1 below as:

TABLE 1. COMPARISON OF DIFFERENT BOTNET DETECTION METHODS

Detection Type	*Detecting Unknown Bot*	*Protocol& Structure Independent*	*Encrypted Bot Detection*	*Real-time Detection*
Signature-based [31]	×	×	×	×
Anomaly-based [32]	√	×	√	×
[33]	√	×	√	×
DNS-based [34]	√	√	√	×
[35]	√	×	√	√
[36]	√	×	√	×
Mining-based [37]	√	×	×	×
[38]	√	√	√	×
[39]	√	√	√	×

5 SDN Defense Mechanism against Botnets

Detection approaches used on conventional networks are generally based on the network traffic habits and patterns.[40] has discuss the detection of 5 main components of P2P botnets with the following explanation as:

i. *Traffic Flow and Feature Extractor Module*: At this stage, network traffic from various hosts is categorized in order to obtain information from network flow.,y7
    a. Creating Detection Model and Training set
    b. Selecting Feature
    c. Classifier
    d. Analyzing Traffic

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

ii. *Report to OpenFlow Controller:*If the detection agent's classification output matches the category on the P2P botnet, the detection agent must notify the arbitrator to change the flow entries in the bridges on the data link.

iii. Flow Rule Modify on OpenFlow Switch: After receiving a Restfull HTTP request from the detector, a Restfull HTTP request in the data-link bridges will alter the flow table.

iv. Drop, Forward, or Redirect Packet

Figure 9discuss the bot detection sequence diagram, following the work phases mentioned below in the figure 8 [40]:

i. Flow Tables initialization
ii. Sending registering packet
iii. Sending Packet-in
iv. Adding new flow rules to mirror
v. Network traffic from P2P botnet generation
vi. Mirror Packets
vii. Result analysis via Restful API

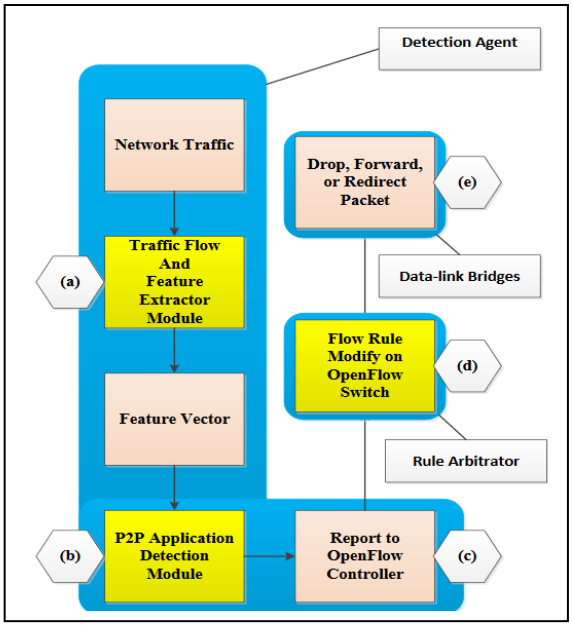
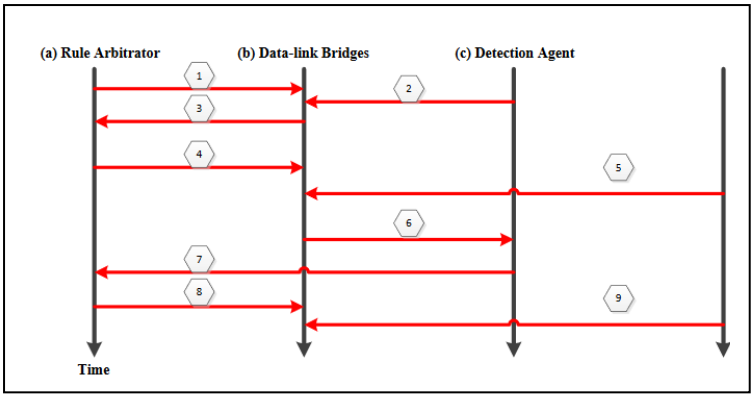


Fig. 8: Botnet detection flow diagram of SDN



ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Fig. 9: Sequence Diagram of Bot Detection

6 Conclusion and Future Scope

Botnets represent a noteworthy danger against digital security as they give a platform to numerous malicious activities or attacks. For example, DDoS attack, malware spread, phishing, and information theft. In spite knowing about theharmful and dangerous effects of botnets, only few proper examinations have analyzed the botnet issues. The process of detecting the presence of botnet is still in its earliest stages. This paper give emphasis on botnet and its discovery.

As discussed above, the high quality of Botnets is a challenge to analyze the botnet by using a multi-tier control systemand command architecture (C&C). Distinction of protocols and structures of botnets makes the process of detecting botnet a very difficult task.Techniques based on signatures can detect only previously known botnets. While unknown bots can be identified by the other groups. As perthe comparison done above, the new data mining-based botnet detection techniques along withDNS-based botnet identification way can identify botnets with a low bogus positive rate in spite of protocol and structure of botnet.The most efficient way to counter the botnet risk to digital environments and software resources was the development of data mining and DNS traffic techniques for exposing botnet C&C traffic.

Moreover, SDN design that isolates the elements of the control criteria and information resources, gives preferences on different sides, the simplicity of modifying the working of the system framework by programming the system-based elements of the system, the cost proficiency of advancement and system improvement, and giving chances to adjustment of new innovation improvements to SDN.In any case, the quality of SDN security framework research is still low at the moment, as proven by the absence of research that tends to the barrier parts of the variety of assaults on SDN arrange security. Also, there is limited scope for tools used for controlling variants of attacks, this paper is dedicated to variations of aBotnet attack. Managing botnets with the honeypot framework is one of the most possible botnet control security tools.

References

[1] B. Saha and A, Gairola, “Botnet: An overview”, CERT-In White PaperCIWP-2005-05, 2005.

[2] M. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, “A multifaceted approach to understanding the botnet phenomenon,” *ACM SIGCOMM Conference on Internet Measurement (IMC)*, pp. 41–52, 2006

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[3] N. Ianelli and A. Hackworth, “Botnets as a vehicle for online crime,” CERT Request for Comments (RFC) 1700, December 2005.

[4] [Online] Honeynet Project and Research Alliance. Know your enemy: Tracking Botnets, March 2005. Available: http://www. honeynet.org/papers/bots/.

[5] F. Hu, Q. Hao and K. Bao, “A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation”. *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2181–2206, 2014”

[6] Samta, Rajni, and S. Kumar, "Speculative Study on DDoS Security Threats in Software Defined Networks." *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 8, no. 8 , August 2019.

[7] D.Kreutz, F.Ramos, P.Verissimo, C.Rothenberg, S.Azodolmolky and S. Uhlig, “Software-Defined Networking: A Comprehensive Survey.” *Proceedings of the IEEE*, vol.103, no. 1, pp. 14-76, December 2014.

[8] R.Hadiantoand T.W.Purboyo, “A Survey Paper on Botnet Attacks and Defenses in Software Defined Networking”, *International Journal of Applied Engineering Research*, vol. 13, no. 1, pp.483-489, 2018

[9] S.Hong,R.Baykov, L.Xu, S. Nadimpali, and G.Gu, “Towards SDN-Defined Programmable BYOD (Bring Your Own Device) Security”, *NDSS*, February 2016.

[10] S. Shin, Wang, and G.Gu, “First Step Toward Network Security Virtualization: From Concept to Prototype”, *IEEE Transaction on Information Forensics and Security*, 2015.

[11] M.Mitchiner, “Software-Defined Networking and Network Programmability: Use Cases for Defense and IntelligenceCommunities” CISCO White Paper, 2014.

[12] S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. Guand M. Tyson, “FRESCO: Modular ComposableSecurity Services for Software Defined Networks” *Proceedings of the 20thAnnual Network and Distributed System Security Symposium (NDSS)*, 2013.

[13] J. Sonchack, A. J. Aviv, E. Keller, and J. M. Smith, “Enabling Practical Software Defined Networking Security Application with OFX”, *NSDI*, 2016.

[14] S. Scott-Hayward, S.Natarajan, and S. Sezer ,“A Survey of Security in Software Define Network” , *IEEE Communication Surveys & Tutorials*, vol.18, 2016

[15] S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake and J. Finnegan, “Are we ready for SDN? Implementation challenges for software-defined networks”, *IEEE Communications Magazine*, vol. 51, pp. 36-43, 2013.

[16] N.Ianelli and A. Hackworth, “Botnets as a vehicle for online crime,” *CERT Request for Comments (RFC)*, vol.1700, December 2005

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[17] Hossein, R. Zeidanloo, Azizah, A. Munaf, "Botnet Command and Control Mechanism", *International Conference on Computer and Electrical Engineering*, 2009.

[18] K.K.R.Choo, "Zombies and Botnets," *Trends and issues in crime and criminal justice*, no. 333, Australian Institute of Criminology, Canberra, March 2007.

[19] D.Dagon, G.Gu, C.P.Lee, W.Lee, "A Taxonomy of Botnet Structures," *Annual Computer Security Applications Conference (ACSAC*), pp. 325-339, 2007

[20] P.Vixie, S.Thomson, Y.Rekhterand J.Bound, [Online] "Dynamic updates in the domain name system(dns update)" Available: http://www.faqs.org/rfcs/rfc2136.html/, 1997

[21] Z. Chi and Z. Zhao, "Detecting and Blocking Malicious Traffic Caused by IRC Protocol Based Botnets", *IFIP International Conference on Network and Parallel Computing Workshop*, 2007.

[22] Hsiao, Han-Wei, S.Tung, M.Shih, and W.Sung, "Using Botnet structure to construct the communication system of a real-time monitoring platform: Botnet structure for real-time monitoring platform", *International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD*), pp. 2860-2865, 2017.

[23] J.B.Grizzard, V.Sharma and C.Nunnery, "Peer-to-Peer Botnets: Overview and case study",*Proceedings of the 1st Workshop on Hot Topics in Understanding Botnets (HotBots 2007),* 2007.

[24] Yin, Chuanlong, Y. Zhu, S.Liu, J.Fei, and H.Zhang, "An enhancing framework for botnet detection using generative adversarial networks", *International Conference on Artificial Intelligence and Big Data (ICAIBD)*, pp. 228-234, 2018.

[25] Park, Wonhyung, and S.Ahn, "Performance comparison and detection analysis in snort and suricata environment", *Wireless Personal Communications*, vol. 94, no. 2, pp. 241-252, May 2017.

[26] J.R. Binkley and S.Singh, "An algorithm for anomaly-based botnet detection",*USENIX Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI),* pp 43–48, 2006.

[27] Cid-Fuentes, J.Alvarez, C.Szabo, and K.Falkner, "An adaptive framework for the detection of novel botnets",*Computers & Security,* vol. 79, pp. 148-161, November 2018.

[28] Alieyan, Kamal, M.Anbar, A.Almomani, R.Abdullahand M.Alauthman, "Botnets Detecting Attack Based on DNS Features", *International Arab Conference on Information Technology (ACIT)"*, pp. 1-4. November 2018.

[29] G.Kirubavathi and R. Anitha, "Botnet detection via mining of traffic flow characteristics", *Computers & Electrical Engineering*,vol. 50, pp. 91-101, February 2016.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[30] M.Chatterjee, A. S.Namin and P. Datta. "Evidence Fusion for Malicious Bot Detection in IoT", *IEEE International Conference on Big Data (Big Data*), pp. 4545-4548, December 2018.

[31] Miller, Sean and C.Busby-Earle, "The role of machine learning in botnet detection", *International Conference for Internet Technology and Secured Transactions (ICITST*), pp. 359-364, December 2016.

[32] Yadavalli, K.Teja and S.Rawat, "BotD: A scalable anomaly-based Bot Detection Architecture for securing web services", *IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pp. 69-73, November 2016.

[33] G.Gu, J.Zhang and W.Lee, "Botsniffer: Detecting botnet command and control channels in network traffic," *Annual Network and distributed System Security Symposium (NDSS)*, 2008.

[34] H.Choi, H.Lee and H. Kim, "Botnet detection by monitoring group activities in DNS traffic," IEEE International Conference Computing Information Technology, pp. 715–720, 2007

[35] N.F.A.Ramachandran and D.Dagon, "Revealing botnet membership using dnsbl counter-intelligence", *Proceedings of 2nd Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI)*, 2006.

[36] D.Dagon, "Botnet detection and response.", *OARC workshop*, vol. 2005, 2005.

[37] W. Strayer, D.Lapsley, B.Walshand C.Livadas, "Botnet Detection Based on Network Behavior", *Advances in Information Security(Springer)*, pp. 1-24, 2008.

[38] M.M.Masud, T.Al-khateeb, L.Khan, B.Thuraisingham,K.W.Hamlen, "Flow-based identification of botnet traffic by mining multiple log file",*International Conference on Distributed Frameworks & Applications (DFMA*), Penang, Malaysia, 2008.

[39] Gu, Guofei, R.Perdisci, J.Zhang and W.Lee, "Botminer: Clustering analysis of network traffic for protocol-and structure-independent botnet detection", vol. 139, 2008.

[40] S.Shang-Chiuan , C.Yi-Ren, T.Shi-Chun, and L.Yi-Bing, "Detecting P2P Botnet in Software Defined Networks", *Security and Communication Networks*, 2017.