A Review Paper on Botnet and Botnet Detection Techniques in Cloud Computing

Shahid Anwar
National Skills University Islamabad
32 PUBLICATIONS **347** CITATIONS
SEE PROFILE

Jasni Mohamad Zain
Universiti Teknologi MARA
161 PUBLICATIONS **2,066** CITATIONS
SEE PROFILE

Mohamad Fadli Zolkipli
Universiti Utara Malaysia
71 PUBLICATIONS **714** CITATIONS
SEE PROFILE

Zakira Inayat
University of Engineering and Technology, Peshawar
15 PUBLICATIONS **529** CITATIONS
SEE PROFILE

A Review Paper on Botnet and Botnet Detection Techniques in Cloud Computing

Shahid Anwar[1], Jasni Binti Mohamad Zain[1], Mohamad Fadli Bin Zulkipli[1], Zakira Inayat[2]
[1]Faculty of Computer System and Software Engineering, University of Malaysia Pahang, Malaysia
[2]Faculty of Computer Science and Information Technology, University of Malaya, Malaysia.

Abstract— **Recently, botnets are the most radical of all cyber-attacks and becoming the key issue in cloud computing. Botnets are the network of different compromised computers and/or smartphones. These devices are infected with malicious code by botmaster and controlled as groups. The attackers use these botnets for criminal activities such as DDoS, click fraud, phishing, spamming, sniffing traffic and spreading new malware. The main issue is how to detect these botnets? It becomes more interesting for the researchers related to cyber-security? This motivates us to write a review on botnets, its architecture and detection techniques.**

Keywords- bots, botnet, botmaster, botnet architecture, botnet attacks, detection techniques

I. INTRODUCTION

The sharp increase of the internet in the past era performed to have facilitated a growth in the occurrences of online attacks[1]. At the modern time internet is becoming the essential need of everyone. Today age is the age of cloud computing, which facilitate the users to access and store the data through cloud. Cloud computing is a representation for enabling everywhere, favorable, on-demand network access to a public, private and hybrid shared lake of computing resources like storage, services, server, networks, and application. These services can be provided with minimum management efforts and very quickly. Devices which are connected to the internet are nowadays under the threat of different attacks performing through computer malicious software's [2] [3]. The cloud servers can be accessed through internet, the more use of cloud computing leads the cloud computing toward the more cyber-attacks.

Botnet is one of the supreme dangerous threat to the cyber-security[4] in these all. Botnet is the combination of two terms, Bot stands for Robot and Net stands for Network, the group of compromised infected internet connected devices are called botnet which is controlled by a human known as Botmaster or Botherder[5]. The botmaster control these infected devices remotely through command and control server. Botnet provide the one-to-many relationship mechanism between command and control server and bots, that's why the botmaster use botnet for advertisement, cyber-attacks and so on. Once a device is infected with malicious code, it becomes the part of a botnet, and start working for the botmaster without knowing to the end user. Botnet propagate itself time to time by compromising more and more devices in the form of mobile phones, laptops, PCs and different servers. The numbers of cyber-attacks which are found in the internet nowadays, most users are affected by these attacks are performed through botnet. Botmaster can perform different kind of cybercrime like DDoS, click fraud, phishing fraud, key logging, bit coins fraud, spamming, sniffing traffic, spreading new malware, google AdSense abuse with bots[6].

Nowadays the botnet is becoming the base of all cybercrime which is performed through the internet[7][8]. Botmaster use different methods to infect a user device to make it bot (zombie) like drive by download , email and pirated software's are the most common way of attacks[9][10]. According to the previous research lots of the detection approaches have been proposed. But most of them are focused on the offline detection of botnet; still we need to focus on the real time detection[11].

The existing botnet detection techniques are categorize into two main groups given as Honeynets Based Detection Technique and Intrusion Detection System[12]. Researchers focus on the cyber-security to detect botnets attacks and prevent cloud servers from the botnet attacks. But still research on botnet detection is immature, and need more research to improve data security in cloud computing.

In the remaining sections of this paper, we present literature review, botnet life cycle, architectures, detection techniques, future work and conclusions.

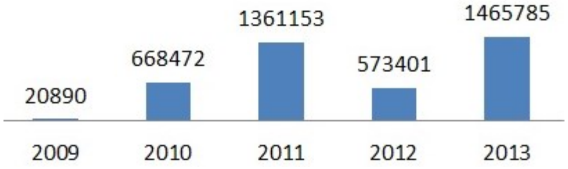

Fig 1: Botnet Drones Attack in Malaysia[14]

The record universal cases performed by botnets are DDoS, click fraud, phishing fraud, key logging, bitcoins fraud, spamming, sniffing traffic, spreading new malware, google AdSense abuse, password stealer and mass identity theft with bots[6]. Like worms propagation the botnet also propagate itself, similarly like virus, botnet also keep it hidden from detection. Botnet has an integrated control and command system that's why it attack similar numerous standardization unaccompanied tools. It spurs with a very high infected by botnet, bots are also known as a zombie, that's why a botnet is also called zombie network.

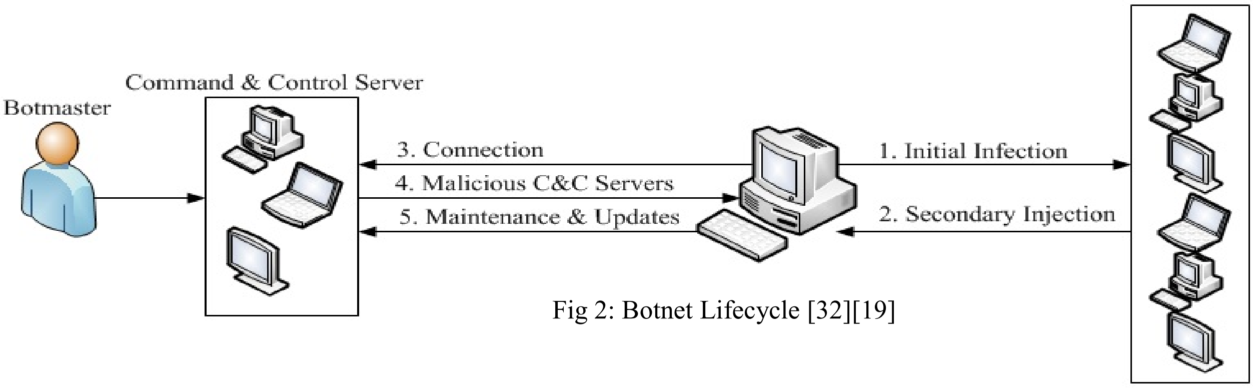

Fig 2: Botnet Lifecycle [32][19]

Cyber criminals start thinking first 1990 to make a botnet for fun, but later their mind was totally changed to make a botnet for profit. Eggdrop was the first botnet created in 1993 [13]. Gtbot and Spybot were created in 2000. Similarly different types of botnets are created in different time slot with more advance techniques and signatures, to secure these botnets from cyber-security. The most dangerous botnet conficker was found in 2009 with the largest number of bots in the history. According to MYCERT (Malaysian Computer Emergency Response Team) statistics report of last five years shows that the botnet drones attacks are increased with a high ratio[14].

II. Botnet Life Cycle

When the botmaster wants to infect another victim device, for this botmaster should go through proper phases, initial infection, secondary injection, connection, sending malicious code and maintenance & updating. First a botnet infect new device connected to the internet, then it inject some malicious code using different protocols like Hyper Text Transfer Protocol (HTTP), FTP and P2P. After successfully injecting the malicious code, the victim device automatically make a connection with already existing command and control server. Once a malicious code is injected to the victim device then it becomes a zombie. In the fourth step the botmaster send commands the bot army through the command and control server [15][6]. This performs malicious activities according to the commands which the victim device receives from the command and control servers [16]. The last step is to maintain and update the zombie active all the time, it send updates to the zombie devices time to time[17][18].

III. Botnet Architectures

The way through which the individual bots form a botnet are classified into three categories according to their architectures. In this paper we introduce some methods of classifying the botnet architectures, and also the advantages and disadvantages are explaining here.

A. Centralized Architecture: Centralized Botnet architecture is the easiest to control and manage by the botmaster. In centralized architecture the botmaster control and supervise all the bots in a botnet from a single central point called command and control server (C&C Server). Thus it's meaning that in centralized botnet architecture all the bots are receive commands and report to a central point called C&C server. There are two types of topologies used in centralized botnet architecture; names are star topology and hierarchical topology. The key protocols are used in centralized architecture are internet relay chat (IRC) and Hyper Text Transfer Protocol (HTTP) [6][19] [20].

Management and monitoring of botnet is very easy because of one central point. The botmaster directly communicate with bots very simply and quickly. In the centralized architecture the design is less complex; while message latency and survivability is low. The botmaster send commands to C&C server from where all these commands are spread in all bots with in a botnet. The main cons of centralized architecture are the failure chances is more than other architecture.

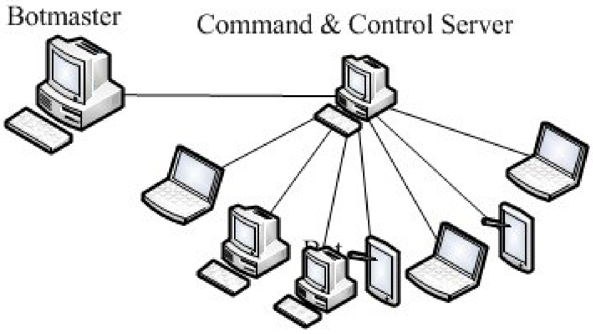

Fig 3: Centralized Botnet Architecture[19][32][31]

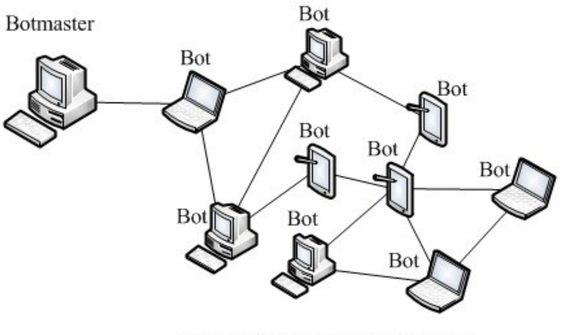

Fig 4: Decentralized Botnet Architecture[19][32][31]

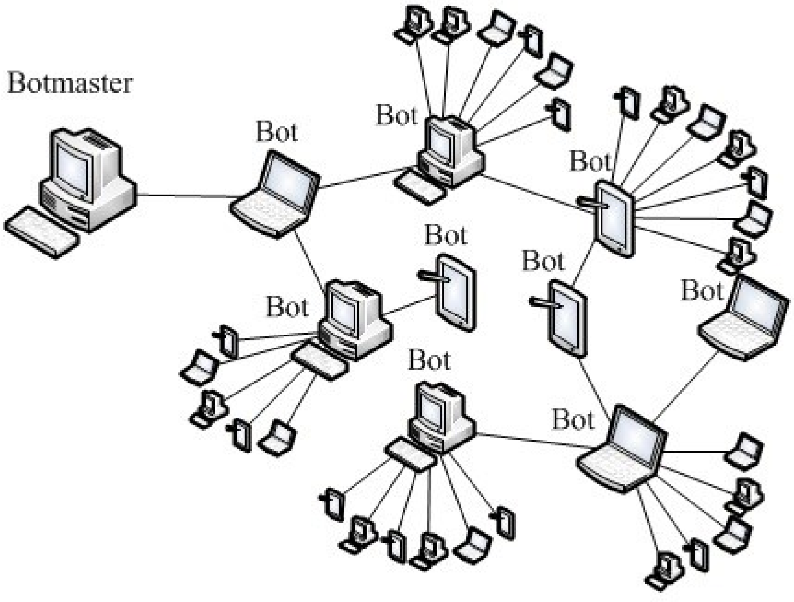

Fig 5: Hybrid Botnet Architecture[19][32][31]

Because of the central point of controlling, if the C&C server becomes failure then all the botnet will be failure[21]. Similarly the detection of botmaster is very easy as compare to decentralize and hybrid architectures [12][22].

B. Decentralized Architecture: In decentralize or peer to peer architecture there is no single entity responsible for controlling the bots in a botnet. There are more than one C&C server which communicate with bots. The detection of such a botnet which using decentralized architecture is harder as compare to centralized architecture. In decentralized architecture there is no specific command and control server; all the bots are acting like a command and control server as well as clients[23].

Decentralized architecture based on the peer to peer protocols. As compare to centralized architecture the design of peer-to-peer architecture is more complex, detection of botnet have such architecture is harder than other botnet. Similarly message latency and survivability is high than centralized botnet architecture. In decentralized architecture the failure chances are less as compare to centralized architecture because if one command and control server becomes failure then the other C&C server can manage and monitor the botnet[22].

C. Hybrid Architecture: Hybrid architecture is the combination of both centralized and decentralized architecture. In hybrid architecture there are two types of bots, one is servant and the other is client bot[24]. The bots are connected to the hybrid botnet either they are client or servant. Monitoring and detection of botnet having hybrid architecture are harder than botnet having centralized and decentralized architectures; while the design is not much complex.

IV. Botnet detection techniques:

Botnet detection is the most important task to improve the cyber-security against various cyber-attacks occurs in internet nowadays. According to the previous research botnet detection techniques can be classified into two categories honeynets detection techniques and intrusion detection techniques [12][25][26]. Intrusion detection system is further divided into sub-categories.

Honeynets& Honeypots Based Detection System: Honeynets and Honeypots both are denoting the end user devices. These end users PC's are the best way to collect critical information about the cyber-attacks. This end user PC is very easy for botmaster to attack and compromise, because it's very vulnerable to malicious attacks. The cyber-security group will be able to make good detection techniques under the collected information about the botnet attacks through these honeynets.

According to the previous research the botnet change their signature time to time because of the security purpose and honeynets are important for understanding these botnet properties [27][28]. In honeynets detection technique honeywall is very important, which is used for monitoring, collecting, modifying and controlling communication over the honeypots.

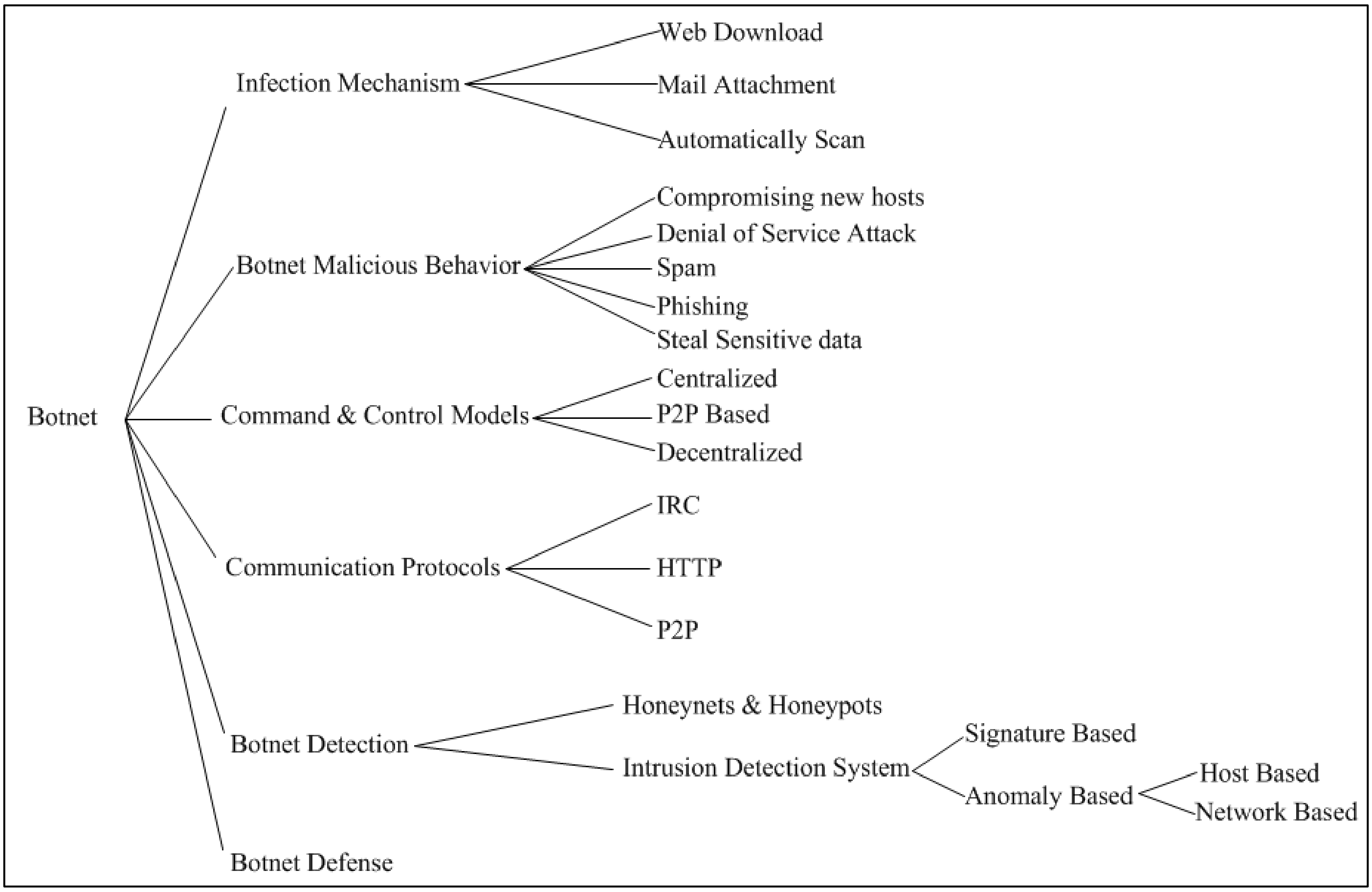

Fig 6: Botnet Taxonomy[31][20]

- *IDS (Intrusion Detection System):* Intrusion detection system is using for monitoring the traffic flow for the malicious activities of a network. During the traffic if it found some malicious attack it directly inform the computer system or the administrator of the system. IDS have also the capabilities to take action against such malicious activities to block the traffic coming from the virus infected system. There are two types of intrusion detection system one is signature based and the other is anomaly based.

A) Signature Based Detection: In signature based botnet detection technique the malware known as the packet sequences or the transportation of the bytes series in seeking network[29]. The key advantage of this detection technique is that signatures are so simple to grow and realize if you know what network performance you're trying to find. This technique is too much simple and easy to understand and develop. The Botmaster change signatures of every attack with time because to make a botnet attack more secure from the bot infected machines[29][30].

B) Anomaly Based Detection: This technique focuses on the idea of criterion for network performance. Anomaly based botnet detection technique can accept only that network activities or traffic which is specified by the administrators or which is feed by the administrator or both in the advance. In this technique the rule should be defined in advance for each protocol and each should be tested for accuracy. It detects those events which not related to the feed or accepted model of performance. Anomaly based detection technique is a little bit expensive according to computation but it is more secure than signature based detection technique. This technique has also some disadvantages in which the main cons is definition of rules is very difficult. For different protocols there are different rules are defined, which are more hard job. Anomaly based technique is also have some limitation about the time and monitoring the bot infected machines [29][31]. This technique is further categorized into network and host based detection techniques.

V. CONCLUSION AND FUTURE WORK

The increasing in number of internet users becomes almost double in the last few years. The more usage of internet leads the users to the cloud computing, while the more use of cloud computing leads the cloud computing to the cyber-attacks. Botnet is one of the biggest cyber-attack nowadays. It distinguishes itself from other malware having the ability to make other machine compromise for a cyber-attack. Botnet propagate itself time to time, and change its shape and signature also with time. Still quarter of the all internet connected computers and smartphones are the part of botnet making different types of criminal activities without knowing to the end users.

In this paper we present detail of botnets, attacks, its different types of architectures, and detection techniques. In all three different architectures it uses different protocols as given in detail. Still detection of botnet is immature; researchers need to do more research on this area. However in future the researcher can do research on the anomaly based botnet detection, making base as high network latency, communication on unusual and usual ports, which indicate the malware.

VI. ACKNOWLEDGEMENTS:

We are thankful to Malaysia Greater Research Network System (MyGRANTS), grant no. RDU 120702, for providing the sufficient funds to conduct this research and for their consent to publish this paper.

REFERENCES

[1] E. Alomari, “Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers : Classification and Art,” vol. 49, no. 7, pp. 24–32, 2012.

[2] M. Thapliyal, N. Garg, and A. Bijalwan, “Botnet Forensics : Survey and Research Challenges,” no. April, 2013.

[3] F. Carpine and S. Maria, “Online IRC Botnet Detection using a SOINN Classifier,” pp. 1351–1356, 2013.

[4] R. A. Rodr, I. Omez, G. M. A-fern, and P. Garc, “Survey and Taxonomy of Botnet Research through Life-Cycle,” vol. 45, no. 4, 2013.

[5] I. Ullah, N. Khan, and H. a. Aboalsamh, “Survey on botnet: Its architecture, detection, prevention and mitigation,” *2013 10th IEEE Int. Conf. NETWORKING, Sens. Control*, pp. 660–665, Apr. 2013.

[6] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, “Botnets: A survey,” *Comput. Networks*, vol. 57, no. 2, pp. 378–403, Feb. 2013.

[7] “Botnets The New Threat Landscape White Paper [Threat Control] - Cisco Systems.” .

[8] M. Zahid, A. Belmekki, and A. Mezrioui, “A new architecture for detecting DDoS/brute forcing attack and destroying the botnet behind,” *2012 Int. Conf. Multimed. Comput. Syst.*, pp. 899–903, May 2012.

[9] W. Paper, “Anatomy of a Botnet.”

[10] “Microsoft Security Intelligence Report,” vol. 15, 2013.

[11] W. Xianghua and C. Lijun, “Analysis and Design of Botnet Detection System,” *2012 Int. Conf. Comput. Sci. Serv. Syst.*, pp. 947–950, Aug. 2012.

[12] X. Zang, A. Tangpong, G. Kesidis, and D. J. Miller, “Botnet Detection Through Fine Flow Classification,” no. 0915552, pp. 1–17, 2011.

[13] C. Batt, “Eggheads,” *Food Microbiology*, vol. 16, no. 3. p. 211, Jun-1999.

[14] “Malaysian Computer Emergency Response Team.” .

[15] M. Feily, A. Shahrestani, and S. Ramadass, “A Survey of Botnet and Botnet Detection,” *2009 Third Int. Conf. Emerg. Secur. Information, Syst. Technol.*, pp. 268–273, 2009.

[16] I. Lin and C. Peng, “A Survey of Botnet Architecture and Batnet Detection Techniques,” vol. 0, no. 0, pp. 81–89, 2014.

[17] N. Hachem, Y. Ben Mustapha, G. G. Granadillo, and H. Debar, “Botnets: Lifecycle and Taxonomy,” *2011 Conf. Netw. Inf. Syst. Secur.*, pp. 1–8, May 2011.

[18] J. Govil, J. Govil, C. Science, and A. Arbor, “Criminology of BotNets and their Detection and Defense Methods,” pp. 215–220, 2007.

[19] S. Khattak, N. R. Ramay, K. R. Khan, A. A. Syed, and S. A. Khayam, “A Taxonomy of Botnet Behavior ,” vol. 94085, pp. 1–27, 2013.

[20] C. Li, W. Jiang, and X. Zou, “Botnet: Survey and Case Study,” *2009 Fourth Int. Conf. Innov. Comput. Inf. Control*, pp. 1184–1187, Dec. 2009.

[21] M. Bailey, E. Cooke, F. Jahanian, Y. Xu, and A. Arbor, “A Survey of Botnet Technology and Defenses,” 2006.

[22] E. Cooke, F. Jahanian, and D. Mcpherson, “The Zombie Roundup : Understanding , Detecting , and Disrupting Botnets.”

[23] D. Dong, Y. Wu, L. He, G. Huang, and G. Wu, “Deep Analysis of Intending Peer-to-Peer Botnet,” *2008 Seventh Int. Conf. Grid Coop. Comput.*, pp. 407–411, Oct. 2008.

[24] R. Mathew, “A New Generation Peer-to-Peer Advanced Botnet,” no. 2, pp. 53–56, 2011.

[25] H. S. Nair and V. E. S. E, “A Study on Botnet Detection Techniques,” vol. 2, no. 4, pp. 2–4, 2012.

[26] A. Sgbau, “A Review-Botnet Detection and Suppression in Clouds,” vol. 3, no. 12, pp. 1–7, 2013.

[27] M. Abu Rajab, J. Zarfoss, F. Monrose, and A. Terzis, “A multifaceted approach to understanding the botnet phenomenon,” *Proc. 6th ACM SIGCOMM Internet Meas. - IMC ’06*, p. 41, 2006.

[28] T. H. Files, “Botnets: Big and Bigger,” pp. 87–90, 2003.

[29] D. S. Eth-tutor, B. T. Supervisor, and B. Plattner, “Signature-based Extrusion Detection,” no. August, 2008.

[30] K. M. C. Tan, K. S. Killourhy, and R. A. Maxion, “Undermining an Anomaly-Based Intrusion Detection System Using Common Exploits,” pp. 54–73, 2002.

[31] C. Liu, C. Peng, and I. Lin, “A Survey of Botnet Architecture and Batnet Detection Techniques,” vol. 16, no. 2, pp. 81–89, 2014.

[32] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, “Botnets: A survey,” *Comput. Networks*, vol. 57, no. 2, pp. 378–403, Feb. 2013.