Botnet Detection Techniques and Research Challenges

Conference Paper · March 2019

DOI: 10.1109/ICRAECC43874.2019.8995028

2 authors:

Sudhakar K.
Jawaharlal Nehru University
5 PUBLICATIONS **7** CITATIONS
SEE PROFILE

Sushil Kumar
Jawaharlal Nehru University
84 PUBLICATIONS **723** CITATIONS
SEE PROFILE

Botnet Detection Techniques and Research Challenges

Sudhakar*
School of Computer & Systems Sciences
Jawaharlal Nehru University
New Delhi-110067, India
Indian Computer Emergency Response Team
MEIT, Government of India
New Delhi-110003, India
Email: $sudhak82\_scs@jnu.ac.in$

Sushil Kumar
School of Computer & Systems Sciences
Jawaharlal Nehru University
New Delhi-110067, India
Email: $skdohare@mail.jnu.ac.in$

***Abstract*—The botnet, a network of compromise internet connected devices, controlled by an attacker are considered to be the most catastrophic cybersecurity threat. In the large-scale cyberattacks, such as DDoS (Distributed Denial-of-Service), spamming, phishing, malware distribution using compromised websites, and malvertisement accomplished with the help of the bot army. This could affect the large enterprises as well as small enterprises. In this paper, we will be discussing the botnet detection techniques, based on their propagation and communication methods. Also, I have identified the various parameters at the network level for the detection purpose. Which are mentioned in the research challenges with some research problems.**

***Index Terms*—Botnet, Cybersecurity, Cybercrime, Honeynet.**

I. Introduction

The machines, connected to the Internet are compromised with the malicious program and formed an illegitimate network, remotely controlled by the bot-master or bothered [1], [2], [3]. The compromised machines are regularly abused by the bot-master to perform their criminal activities through the Internet.

Initially, the bots have developed *from the subject of curiosity to highly sophisticated instruments* for the cybercriminal [4]. The idea of the botnet was originated from Internet Relay Chat (IRC), currently known as IRC protocol [5]. A simple text-based was a chatting software that systematize the communication in channels. At that time, the bots were not designed to harm the system. The primary purpose of the botnet was to manage and interact with their fellow IRC chat room members. Members could decode the simple command issued by the controller to provide administrative assistance, gather information about the user and operating system, login information, email, and aliases.

Eggdrop was the first IRC bot published in 1993 [6] and improved with additional features. The improved IRC bots were capable of attacking their fellow IRC users, and it could also attack the entire server.

With the evolution of new bots, more complex mechanisms of communication with the bot-master were developed that exploits other available protocols, these sophisticated techniques made bot more powerful. Now, they have the capability to spread like a worm, hide in the system like virus and Trojan, able to download more malware, launch massive and coordinated attacks as represented in Fig 1.
The new generation of bots adapting new techniques to propagate−

- Some malware will come in handy with email attachments when a user clicks on the attachment it downloads and executes itself.
- The bots were propagating through infected websites, just visiting those websites might download a malicious program
- Some systems were not properly patched and updated with the latest security updates have some old vulnerabilities; the bot-master could use exploits those vulnerabilities to create a back-doors to control the host remotely.
- The code injection techniques used by an attacker to distribute the malware through the Internet by injecting the malicious code in a file like a document file, images, PDF, etc.
- Communication protocol could also be exploited to distribute malware such as IRC, HTTP, and P2P.
- Malware infiltrates by exploiting web-based vulnerabilities and take control of the targeted systems.

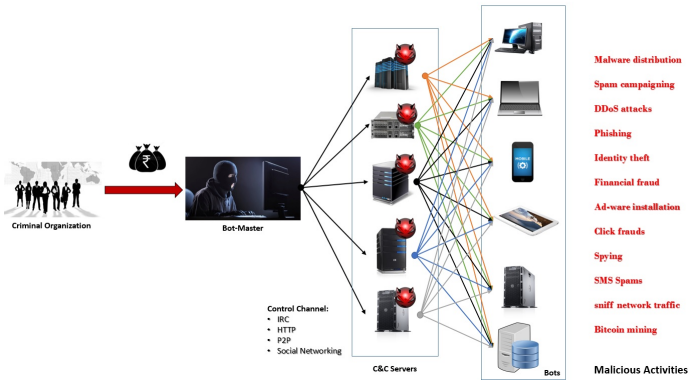

Fig. 1. The graphical representation of malicious activities of Botnet.

A. Defining Bot and Botnet

Widely varying the definition of the bot and botnet have emerged [7]. However, the term comprehensibly defines active bots, connected to the command and control (C&C) server that are controlled/managed by botmaster. Communication plays a vital role among bots, botmaster, and C&C. But, In the case of malware infection, the capability of malware to connect with other malicious instance is not sufficiently classified as a part of a botnet. Therefore, necessary two conditions must be met to become a bot from the compromised machine:

1) Remotely controllable: A bot-master always be able to control a bot remotely through the communication channel by giving some commands. The level of control depends on up-to what extent the attacker has gain access to the compromised system.

2) Adaptable: The adaptation feature already included int he bot source code to update or upgrade. The bot-master can control the adaptation by the C&C server that can further used to migrate the C&C to downloads of new settings and malware. These two conditions are required to pre-build modules to do the respective job in any bot.

B. Different types of Botnet

1) IRC-based Botnet: IRC is a protocol designed for real-time text-only communication between the bots. According to Silva et al. [6], IRC-based botnet was the first generation of the botnet. Bots in this type of botnet connect to an IRC server created by the bot-master and wait for commands. The bot-master can control bots through C&C server by issuing control commands to perform criminal activities by its bot army [6], [8], [9].

2) HTTP-based Botnet: The botnet-controlled via the HTTP-based C&C server by the bot-master through some specific commands. The use of encryption can ensure the anonymity over the communication channel. The commands are issued via a website, or C&C maintained by the bot-master. Bots periodically query this website for new commands, enclosed in HTTP response objects [10].

3) Peer-to-Peer (P2P) Botnet: Traditionally, the botnet is organized hierarchically with a C&C server. This server location can be written in the bot module, or the directory server can define it at the time of a request. Presently, the centralized C&C is useful for the security professionals to take-down these C&C. To overcome this failure, one class of botnet structure that has entered the initial stages of development is P2P based architectures. In this architecture of botnet makes even more challenging to track-down the C&C server for security experts because of the P2P design every host/bot have the capability to become a host or server [11].

C. Infection Life Cycle of the Botnet

In order to become the part of a botnet, a bot has to go through a cycle of phases so that the compromised host be useful as botmaster may desire. These phases may have different names in different literature's but some are well described in [8], [9], [6] as in Fig 2.

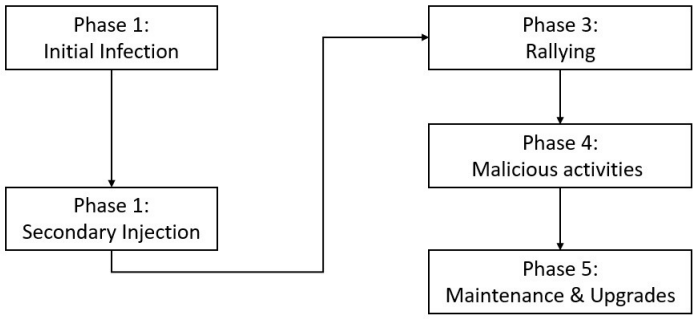

Fig. 2. The life cycle of a Botnet.

1) Initial infection: A host can be infected in many ways-

- A malicious program able to exploits some vulnerability in the host system in order to gain user privileges of the system.
- Malware automatically downloaded at the time of visiting malicious websites.
- Malware can be reached to the host system by email attachment.
- Malware can be distributed by the USB autorun.

2) Secondary injection: The malware downloaded in initial infection, now download the original bot program and run in the host machine to become an active host by connecting with its C&C server. A bot could be download via FTP, HTTP, and P2P.

3) Rallying: Once the bot successfully infiltrates the victim's machine, it typically informs the botmaster (or peers in case of P2P C&C channel) about joining the botnet.

4) Malicious activities: The army of bots gets commands/instructions from its bot-master through C&C server for conducting malicious activities as described in [8], [6] and graphically represented in Fig 1.

5) Maintenance and upgrade: The bots are needed to be upgraded periodically to become more resilient and undetected.

II. Detection of Botnet C&C Servers - A Literature Survey

Detection techniques of the botnet are one of the most important issues should be taken when combating network security threads because botnet gives the potential power to conduct various malicious activities as well as cybercrimes. So researcher must have developed and proposed some detection techniques described in [9], [12], [13].

According to the previous study [13], the detection techniques can be further divided into two categories; one is *honeynet-based detection* and second is *Intrusion Detection Systems* (IDSs).

1) ***Honeynet-based:*** This technique is meet the requirement of the detection and the collection of the bot binaries [14], [1], [15], [16], [17]. It is mainly used in monitoring and strengthening the cyber defense system [16], [17].
2) ***Intrusion Detection Systems:*** The system is further classified as *(a). signature-based detection* and *(b). anomaly-based detection*.

(a). Signature-based detection technique can apply only for the pre-defined signature of well-known bots into IDS detection system [18], [19], [20]. Consequently, this mechanism does not work on unknown bots and the system fails to detect some bots with a slightly different signature. ***(b). Anomaly-based detection*** is the idea to detect bots through identifying the anomalies in the network traffic including high network latency, traffic on unusual ports and high network volume shows the existence of malicious bots in the network [21], [22]. The network based detection can be divided in to *host-based detection* and *network-based detection techniques*.

A. Host-based detection

In the host-based detection techniques, need to analyze the behavior of the individual machine by analyzing their process activities on the systems (*e.g.*, registry changes, file system changes, a connection made for external communication, etc.) are different from the changes made by legitimate processes [23], [22].

Masud et al. [24] the mining algorithms applied to multiple log files in the flow-based network traffic to identify the C&C by which bots are communicating with their master. The response of the machine and human are recorded in the host-based log file that could be analyzed to distinguish the request made by machine or human, which can be further used to detect the bot-generated traffic and benign traffic with the help of proposed log correlation by the author. The log correlations can also be used to identify non-IRC botnet.

In the proposed model [25] a tool *BotTracer* is developed to detect the trivial three phases life-cycle of bots by using the virtual machine techniques. Three passes of the life-cycle are- ***Startup:*** after the successfully in-plantation of the bot to the compromised system, it runs automatically; ***Prepare:*** connect with its C&C and ready to receive commands; and ***Attack:*** botmaster will issue the attack command through C&C to perform the malicious activities as mentioned in the Fig 1.

A security tool *DeWare* [26] has been developed for the detection of malware infection at the host level in the initial phase by enforcing the properties of operating systems such as process control system and file system. The tool has the capability to detect drive-by download as well as browser-based exploits.

B. Network-based detection

Although there are so many detection techniques available on the literature [2], the behaviour of a bot is changing very frequently than the traditional malware. Therefore it is difficult to detect it effectively. Some evasion techniques are commonly used by the botnet to become undetected.

- **Encryption-** The network traffic is similar whether it is bot generated traffic or legitimate traffic and to evade the detection mechanism it may use encryption techniques.
- **Fast-flux-** This technique is used to evade the detection mechanism.

Malicious actor, the Bot could be detected by monitoring the network traffic [27]. The network-based monitoring can be classified into two categories; Real-time monitoring which is referred as ***active*** monitoring and long-term monitoring as ***passive*** monitoring.

1) Active monitoring: In [28] the paper, the *active* monitoring technique *BotProbe* was implemented to identify the bot generated traffic while communicating with botmaster.

The technique using response time of botnet communication with their C&C for the detection purpose. The drawback of this approach is having slow detection rate because it requires the observational input from the following phases - various infection stages (*BotHunter*) [29], various instances/rounds of communications/activities (*Botsniffer*) [30] and a long communication/activity time (*BotMiner*) [31].

2) Passive monitoring: These techniques are developed to detect any suspicious communication in the network traffic generated by bots in long-term for the detection purpose.

In this monitoring technique, leveraging the similar communication pattern used by bots of same botnet in both centralized and decentralized architecture (e.g., P2P) [23], [31]. In this category the different techniques and methods are being used by researchers such as [27], [32], [33], traffic mining [31], [24], [34], graph theory [35], clustering [33], [36], machine learning [24], group analysis [30], [29], [37].

C. Protocol specific detection

The attacks can be targeted to the specific protocol to infiltrate the host machine and compromised the system with the bot. The detection techniques are developed explicitly for protocols to detect the compromised bots, involving multiple protocols and architectures. Protocol-based detection literature is described below in detail.

1) IRC protocol based detection: The inception of the IRC botnet detection technique was proposed in [1] this, and the structure of the bot and botnet was discussed. The method is focused on the monitoring of IRC communication, and the correlation of the network traffic with the extracted features from infected machines was used to identify the presence of bots in the network.

The signature-based IRC bot detection solution [18], [38] is developed that uses the nickname as a pattern for the detection purpose. The features were included in this system such as odd or suspicious IRC nicknames, IRC servers, and uncommon server ports. The drawback of this system is that it can not detect the encrypted communication or non-IRC botnet.

2) DNS protocol based detection: Choi et al. [2] proposed an anomaly-based detection system by considering the common activities in DNS traffic called BotGAD (Botnet Group Activity Detector). The author also able to detect the migration of C&C server using this detector. The downside of this method is that it requires more computational power to monitor the enormous amount of network traffic adequately [9]. In addition to the above mentioned technique, Villamarín-Salomón and Brustoloni [39] has proposed two different approaches to identify the C&C server through the analysis of DDNS (Dynamic DNS) traffic.

a) The first approach depends on the filtering all domains, which has abnormally high DDNS query rate. It indicates that the botmaster is frequently migrating the C&C server to different IP.
b) In the second approach, the author is trying to decontaminate the unusual recurring DDNS replies. The query indicates that the bot is trying to connect with the C&C server, which has already been taken-down using sink-holing techniques [40].

3) SMTP protocol based detection: Stringhini et al. [41] have developed a tool *BotMagnifier* to detect the spambots over the internet. The tool uses the datasets from *DNSBLs* (Domain Name System based Blackhole Lists) [42] and logs of *spamhaus* [43] to detect the spamming behaviour of the bot.

4) P2P protocol based detection: Zhang et al. [32] proposed a technique to identify the P2P botnet by using statistical fingerprinting of the host engaged in P2P communication. This fingerprint is used to compare the traffic generated by P2P botnet and by the legitimate P2P application. The selection of P2P bot is mentioned in the fig 3, and some important parameters are identified from the network traffic to generate the statistical fingerprinting are listed below−

- TCP/UDP and IP pairs
- (IP, Port) pairs
- Connection responded success rate
- Mean port numbers used to communicate with external host
- Up/Down traffic ratio
- DNS request

Fig. 3. Proposed techniques in phases [32].

D. Multipurpose techniques

Gu, Guofei, et al. [29] developed a complex *"evidence-trail"* approach (i.e. *BotHunter*) to detect the successful bot infection by analysing the initial communication pattern that recorded during the infection process. The infection life-cycle is included target scanning, infection exploit, binary egg download and execution, C&C channel establishment, and outbound scanning. In this approach, the author able to detect the bots using IDS-Driven dialog correlation with the help of two anomaly-detection plug-ins (i.e., SLADE and SCADE) for the botnet detection purpose.

TABLE I
BOTNET DETECTION TECHNIQUES CLASSIFICATION

Communication	Refs
IRC	[1], [13], [14], [18], [38]
DNS	[2], [9], [15], [39], [42], [45], [46], [47], [48]
SMTP	[41], [42], [43]
P2P	[11], [23], [31], [32], [33], [34]

Rieck Konrad et al. [44] presents *Botzilla*, a network monitoring tool that uses horizontal and vertical correlation to detect the malicious behavior of the infected machine. After the successful infection, the malicious program tends to contact its master by a process called *"phoning home"* at that time the signature has been generated. All the communication from the malicious program is being monitored for the signature generation purpose even if the single host is infected.

E. Botnet Detection using Machine Learning

Most of the botnets are using DGAs (Domain Generation Algorithms) to communicate with their botmaster. The security professionals have to reverse engineered the bot sample and extract the DGA algorithm to find out the seed. To detect this type of botnet researchers have proposed the machine learning approach to predict the domains generated by DGA by analyzing the DNS queries [45], [46], [47], [48].

III. RESEARCH CHALLENGES

Many researchers have already proposed various solutions and mechanisms for the detection of the botnet. In this paper, I have identified the different parameters through which the detection on the network level could be possible. The parameters are-

- Every bot has to connect with their C&C to become the part of a botnet, and communicate with botmaster.
- Detection of C&C traffic from the network flow to identify infiltrated bots and its owner.
- Network-based detection has a low dependency on end systems and a little exposure to malware.

The objectives of this paper are to detect C&C server through which botnet communicate with botmaster, C&C is the only link between botmaster and bots if we can want track-down the botmaster we need to identify C&C and then trace back to botmaster. Botmaster used very secure communication channel to hide from the security professionals and law-enforcement agencies. But, it is relatively easy to detect C&C and take-down all the domain related to the C&C at a time to make all bots inactive and destroy the botnet, then communication link between C&C and botmaster will be demolished. Therefore, botmaster no longer has the control to those bots.

Some of the problem related to the detection of the C&C servers are mentioned below which we will pursue in this research.

a) Investigation of the C&C servers involved in botnet communication using behavioral analysis and finding some specific patterns through which the botnet communicate with its C&C to get further instruction from the botmaster.
b) Detection of botnet C&C in the network traffic using protocol-based detection mechanism.
c) Detection of C&C by investigating untrusted destination of DNS request.

IV. Conclusion

In this paper, we have discussed the most dangerous cyberthreat, botnet. The botnet attack can be catastrophic because of its attack vectors and bot army. The article also classifies the botnet, based on their detection strategy and communication channel used in the table I. The botnet can be undetected by using the *encrypted* communication and domain *fast-flux* techniques. The open challenges are given in the research challenges which shall be implemented in the future.

References

[1] E. Cooke, F. Jahanian, and D. McPherson, "The zombie roundup: Understanding, detecting, and disrupting botnets." *SRUTI*, vol. 5, pp. 6–6, 2005.

[2] H. Choi, H. Lee, and H. Kim, "Botgad: detecting botnets by capturing group activities in network traffic," in *Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE*. ACM, 2009, p. 2.

[3] D. A. Girei, M. A. Shah, and M. B. Shahid, "An enhanced botnet detection technique for mobile devices using log analysis," in *Automation and Computing (ICAC), 2016 22nd International Conference on*. IEEE, 2016, pp. 450–455.

[4] C. Czosseck, G. Klein, and F. Leder, "On the arms race around botnets-setting up and taking down botnets," in *2011 3rd International Conference on Cyber Conflict*. IEEE, 2011, pp. 1–14.

[5] en.wikipedia.org. Internet Relay Chat. [Online]. Available: https://en.wikipedia.org/wiki/Internet$_Relay_Chat$

[6] S. S. Silva, R. M. Silva, R. C. Pinto, and R. M. Salles, "Botnets: A survey," *Computer Networks*, vol. 57, no. 2, pp. 378–403, 2013.

[7] M. Fabian and M. A. Terzis, "My botnet is bigger than yours (maybe, better than yours): why size estimates remain challenging," in *Proceedings of the 1st USENIX Workshop on Hot Topics in Understanding Botnets, Cambridge, USA*, 2007.

[8] Z. Zhu, G. Lu, Y. Chen, Z. J. Fu, P. Roberts, and K. Han, "Botnet research survey," in *2008 32nd Annual IEEE International Computer Software and Applications Conference*. IEEE, 2008, pp. 967–972.

[9] M. Feily, A. Shahrestani, and S. Ramadass, "A survey of botnet and botnet detection," in *2009 Third International Conference on Emerging Security Information, Systems and Technologies*. IEEE, 2009, pp. 268–273.

[10] K. Aoki, T. Yagi, M. Iwamura, and M. Itoh, "Controlling malware http communications in dynamic analysis system using search engine," in *Cyberspace Safety and Security (CSS), 2011 Third International Workshop on*. IEEE, 2011, pp. 1–6.

[11] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon, "Peer-to-peer botnets: Overview and case study." *HotBots*, vol. 7, pp. 1–1, 2007.

[12] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang, "Botnet: classification, attacks, detection, tracing, and preventive measures," in *EURASIP journal on wireless communications and networking*, vol. 2009. IEEE Computer Society, 2009, pp. 1184–1187.

[13] H. R. Zeidanloo, M. J. Z. Shooshtari, P. V. Amoli, M. Safari, and M. Zamani, "A taxonomy of botnet detection techniques," in *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, vol. 2. IEEE, 2010, pp. 158–162.

[14] P. Bacher, T. Holz, M. Kotter, and G. Wicherski, "Know your enemy: Tracking botnets," 2005.

[15] D. Dagon, C. C. Zou, and W. Lee, "Modeling botnet propagation using time zones." in *NDSS*, vol. 6, 2006, pp. 2–13.

[16] J. Bethencourt, J. Franklin, and M. Vernon, "Mapping internet sensors with probe response attacks." in *usenix security*, 2005.

[17] C. C. Zou and R. Cunningham, "Honeypot-aware advanced botnet construction and maintenance," in *International Conference on Dependable Systems and Networks (DSN'06)*. IEEE, 2006, pp. 199–208.

[18] J. Goebel and T. Holz, "Rishi: Identify bot contaminated hosts by irc nickname evaluation." *HotBots*, vol. 7, pp. 8–8, 2007.

[19] Y. Kugisaki, Y. Kasahara, Y. Hori, and K. Sakurai, "Bot detection based on traffic analysis," in *Intelligent Pervasive Computing, 2007. IPC. The 2007 International Conference on*. IEEE, 2007, pp. 303–306.

[20] P. Wurzinger, L. Bilge, T. Holz, J. Goebel, C. Kruegel, and E. Kirda, "Automatically generating models for botnet detection," in *European symposium on research in computer security*. Springer, 2009, pp. 232–249.

[21] B. Saha and A. Gairola, "Botnet: an overview," *CERT-In White Paper, CIWP-2005-05*, vol. 240, 2005.

[22] J. R. Binkley and S. Singh, "An algorithm for anomaly-based botnet detection." *SRUTI*, vol. 6, pp. 7–7, 2006.

[23] T. Micro, "Taxonomy of botnet threats," *Whitepaper, November*, 2006.

[24] M. M. Masud, T. Al-khateeb, L. Khan, B. Thuraisingham, and K. W. Hamlen, "Flow-based identification of botnet traffic by mining multiple log files," in *Distributed Framework and Applications, 2008. DFmA 2008. First International Conference on*. IEEE, 2008, pp. 200–206.

[25] L. Liu, S. Chen, G. Yan, and Z. Zhang, "Bottracer: Execution-based bot-like malware detection," in *International Conference on Information Security*. Springer, 2008, pp. 97–113.

[26] K. Xu, D. Yao, Q. Ma, and A. Crowell, "Detecting infection onset with behavior-based policies," in *Network and System Security (NSS), 2011 5th International Conference on*. IEEE, 2011, pp. 57–64.

[27] A. V. Barsamian, "Network characterization for botnet detection using statistical-behavioral methods," Ph.D. dissertation, Dartmouth College, 2009.

[28] G. Gu, V. Yegneswaran, P. Porras, J. Stoll, and W. Lee, "Active botnet probing to identify obscure command and control channels," in *Computer Security Applications Conference, 2009. ACSAC'09. Annual*. IEEE, 2009, pp. 241–253.

[29] G. Gu, P. A. Porras, V. Yegneswaran, M. W. Fong, and W. Lee, "Bothunter: Detecting malware infection through ids-driven dialog correlation." in *Usenix Security*, vol. 7, 2007, pp. 1–16.

[30] G. Gu, J. Zhang, and W. Lee, "Botsniffer: Detecting botnet command and control channels in network traffic," 2008.

[31] G. Gu, R. Perdisci, J. Zhang, W. Lee *et al.*, "Botminer: Clustering analysis of network traffic for protocol-and structure-independent botnet detection." in *USENIX Security Symposium*, vol. 5, no. 2, 2008, pp. 139–154.

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

[33] D. Liu, Y. Li, Y. Hu, and Z. Liang, "A p2p-botnet detection model and algorithms based on network streams analysis," in *Future Information Technology and Management Engineering (FITME), 2010 International Conference on*, vol. 1. IEEE, 2010, pp. 55–58.

[34] W.-H. Liao and C.-C. Chang, "Peer to peer botnet detection using data mining scheme," in *Internet Technology and Applications, 2010 International Conference on*. IEEE, 2010, pp. 1–4.

[35] M. Iliofotou, P. Pappu, M. Faloutsos, M. Mitzenmacher, S. Singh, and G. Varghese, "Network monitoring using traffic dispersion graphs (tdgs)," in *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*. ACM, 2007, pp. 315–320.

[36] F. Yu, Y. Xie, and Q. Ke, "Sbotminer: large scale search bot detection," in *Proceedings of the third ACM international conference on Web search and data mining*. ACM, 2010, pp. 421–430.

[37] R. Sharifnya and M. Abadi, "Dfbotkiller: domain-flux botnet detection based on the history of group activities and failures in dns traffic," *Digital Investigation*, vol. 12, pp. 15–26, 2015.

[38] P. A. A. Resende and A. C. Drummond, "Http and contact-based features for botnet detection," *Security and Privacy*, vol. 1, no. 5, p. e41, 2018.
[39] R. Villamarín-Salomón and J. C. Brustoloni, "Identifying botnets using anomaly detection techniques applied to dns traffic," in *2008 5th IEEE Consumer Communications and Networking Conference*. IEEE, 2008, pp. 476–481.
[40] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, "Your botnet is my botnet: analysis of a botnet takeover," in *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009, pp. 635–647.
[41] G. Stringhini, T. Holz, B. Stone-Gross, C. Kruegel, and G. Vigna, "Botmagnifier: Locating spambots on the internet." in *USENIX Security Symposium*, 2011, pp. 1–32.
[42] A. Ramachandran, D. Dagon, and N. Feamster, "Can dns-based blacklists keep up with bots?" in *CEAS*. Citeseer, 2006.
[43] Spamhaus. (2019, January 04). [Online]. Available: https://www.spamhaus.org/
[44] K. Rieck, G. Schwenk, T. Limmer, T. Holz, and P. Laskov, "Botzilla: Detecting the phoning home of malicious software," in *Proceedings of the 2010 ACM Symposium on Applied Computing*. ACM, 2010, pp. 1978–1984.
[45] J. Woodbridge, H. S. Anderson, A. Ahuja, and D. Grant, "Predicting domain generation algorithms with long short-term memory networks," *arXiv preprint arXiv:1611.00791*, 2016.
[46] P. Lison and V. Mavroeidis, "Automatic detection of malware-generated domains with recurrent neural models," *arXiv preprint arXiv:1709.07102*, 2017.
[47] H. Mac, D. Tran, V. Tong, L. G. Nguyen, and H. A. Tran, "Dga botnet detection using supervised learning methods," in *Proceedings of the Eighth International Symposium on Information and Communication Technology*. ACM, 2017, pp. 211–218.
[48] D. Tran, H. Mac, V. Tong, H. A. Tran, and L. G. Nguyen, "A lstm based framework for handling multiclass imbalance in dga botnet detection," *Neurocomputing*, vol. 275, pp. 2401–2413, 2018.