PHYSICAL SCIENCES

ISSN (Print): 24490954
ISSN (Online): 26364972

PEER-TO-PEER BOTNETS: A SURVEY ON PROPAGATION, DETECTION AND DETECTION EVASION TECHNIQUES

[1]Oyelakin, A.M.,[2] Salau-Ibrahim, T.T., [3]Ogidan, B.S., [4]Azeez, R.D., [5]Ajiboye, I.K.

[1] Computer Science Unit, Department of Science Education, Al-Hikmah University, Ilorin, Nigeria.
[2,,3] Department of Computer Sciences, Al-Hikmah University, Ilorin, Nigeria.
[4] ICT Unit, Al-Hikmah University, Ilorin, Ilorin, Nigeria
[5] Computer Science Department, Abdul-Raheem College of Advanced Studies
(An Affiliate of Al-Hikmah University, Ilorin, Nigeria)

Corresponding Email: amoyelakin@alhikmah.edu.ng

Manuscript Received:11/12/2018 Accepted:20/12/2019 Published: December 2019

ABSTRACT

Botnets have been identified as one of the major threats to users in the internet space, nowadays. Unlike other categories of malware, botnets use Command and Control channels to launch and propagate their attacks. These botnets have been classified as centralised and decentralised (Peer-to-Peer). Due to the structure, Peer-to-Peer botnets have different behavioural characteristics from centralised botnets. Past researches have equally identified that Peer-to-Peer botnets are more difficult to detect and shutdown compared to centralised botnets. This work provides a survey on the propagation, detection and detection evasion techniques of Peer-to-Peer botnets. The study was able to identify various machine learning-based classifiers that have been proposed to detect Peer-to-Peer botnets in the cyber space. It is believed that any identified gap in the detection mechanisms will bring better insights into P2P botnet researches. The work concluded that identifying some of the Peer-to-Peer botnet propagation mechanisms and their detection evasion techniques will enable security researchers and experts to come up with improved botnet identification and mitigation approaches.

Keywords: Peer-to-Peer Botnets, Evasion Techniques, Malware, Adversarial Attacks, Botnet Detection

INTRODUCTION

A Botnet is a network of malware-infected computers that are being controlled by an attacker through the use of Command and Control (C&C) channel (Martinez-Bea, Castillo-Perez, & Garcia-Alfaro, 2013; Zand, Vigna, Yan, and Kruegel, 2014). Botnets are fast becoming the most serious threats in the internet space (Barford and Yegneswaran, 2006.; Ping, Lei, Baber and Cliff, 2014;Fergusion, 2018; Muhammad, Manjinder, and Ashraf, 2013; Bbarthakur, Dahal and Ghose, 2013; Shirley, Lokesh and Chad, 2012.; Grizzard., Sharma, Nunnery, Byung, Kang and Dagon, 2007). With a growing increase in these botnet attacks, computer networks are constantly under threat from attacks that cripple cyber-infrastructure (Santana, Suthaharan and Mohanty, 2018). The cyber attackers use several variants of malware to launch sophisticated attacks in the cyber space. A malware is a kind of software that is used for performing malicious attacks and network intrusions (CERT, 2002; Ping, *et al.,* 2014). The common categories of malware include: viruses, worms, Trojan horses, botnets and so on. It has been identified that botnets are used to launch attacks such as drive by download, phishing, and click fraud and so on (Ianelli and Hackworth, 2005; Alparslan *et al.,* 2012; Nicholas and Aaron, 2005) mostly for financial gains.

Rajab, Zarfoss, Monrose, and Terzis (2006) have argued that modern bots are equipped with several exploit vectors to improve opportunities for exploitation. Through the use of Command and Control (C&C) Channels, botnets are being controlled and updated by the botherders. Wang, Aslam and Zou (2010) classified Peer-to-Peer botnets into Parasite P2P botnet, Leaching P2P botnet, and Bot-only P2P botnet. For the purpose of identifying intrusion in a network or system, (Rawat, Pilli and Joshi, 2018) classified botnet detection methods into Honey-based and IDS-based as shown in Figure 1. Peer-to-Peer botnets are new variants of botnets that operate based on Peer-to-Peer architecture. In a P2P network, every node can act as a server and as a client. This is why the take down attempt of P2P botnet is difficult.

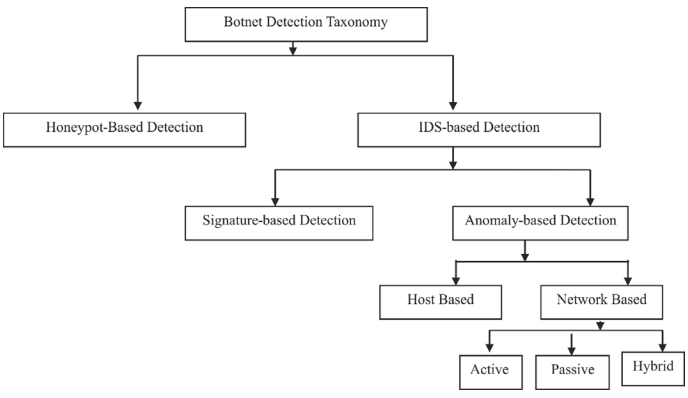

Figure 1: Taxonomy on Botnet Detection Techniques (Rawat, Pilli and Joshi, 2018)+

MATERIALS AND METHODS

Materials

The materials used in this are collection of relevant literature on Peer-to-Peer botnets detection. Emphasis is on having a better understanding of these kind of botnets that have been reported to be more resilient compared to centralized botnets.

Methods

The method used in this work is a survey approach. The work reports some of the identified literature based on the propagation mechanism, the detection models as well as detection evasion techniques of Peer-to-Peer botnets. There has been paucity of work on the survey of evasion techniques used by Peer-to-Peer botnets. With the growing appearance of botnet malware in the cyber space, understanding the propagation and detection evasive techniques of peer-to-peer botnets as examples of new variant of botnets is becoming more relevant.

A Survey on Peer-to-Peer Botnet Propagation Mechanism

A shift in the architecture of botnets from centralised to decentralized make the study of Peer-to-Peer botnet architecture to be very prominent as detection and mitigation are more challenging. Hence, Mimoso, 2013; Alauthaman, Aslam, Zhang, Alasem, Hossain (2018) pointed out that the emergence of P2P botnets has made botnet detection to be a very big challenge when compared to centralised botnets. Botnet Command and Control (C&C) techniques that are used to operate botnets remotely operate in peer-to-peer basis in a P2P botnets. Generally a botnet is propagated by first of all identify the vulnerable systems as well as the tools to exploit them. Then, these tools are used to gain backdoor access to the targeted systems (Banday, Qadri and Shah, 2009). This process facilitates the installation of bot malware by uploading or commanding the victim machine to download a copy of the bot (Shannon and Moore, 2004). This infection stage involves use of various direct and indirect techniques to spread bot malware. These include attacks through software vulnerabilities, vulnerabilities caused by other infections, social engineering through the use of email, instant messaging and malicious web page content.

Specifically, the bot malware is also propagated through peer to peer networks, open file sharing, and direct client to client file exchange. The malware uses FTP, TFTP, HTTP protocol based services to infect computers and spread it until a desired strength of botnet is assembled (Choo, 2007). Feily et al. (2009) divides the life-cycle of a botnet into five distinct phases: initial infection, secondary injection, connection, malicious command and control, and update and maintenance. The work reported that at the initial infection phase, an attacker exploits a known vulnerability for a target system and infects the victim

device, and then grant additional capabilities to the attacker on the target system. The work pointed out that in the secondary injection stage, the attacker uses his newly acquired access to execute additional scripts which then fetch a malicious binary from a known location. Once the binary has been installed, the victim computer executes the malicious code and becomes a bot. In the connection phase, the bot attempts to establish a connection to the command and control server through a variety of methods, joining the botnet officially once this connection has been established. The maintenance phase is the last phase of the botnet lifecycle, bots are commanded to update their binaries, typically to defend against new attacks or to improve their functionality. Similarly, Leonard *et al.* (2009) divides a botnet's lifecycle into four phases: formation, C&C, attack and post-attack. As mentioned by David *et al.* (2013), the attack phase is noted as a phase in the botnet lifecycle when the bot is actively performing malicious activities based on received instructions, while the post-attack phase is similar to the maintenance phase described by Feily *et al.* (2009). The Communication structure of botnet is as shown in Figure 2.

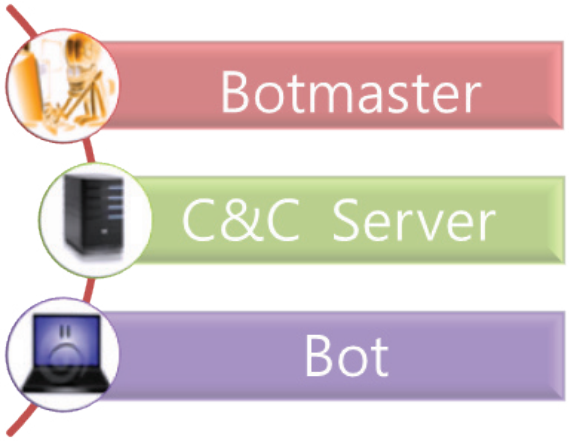

Figure 2: Botnet Communication Structure (Zhiqi, Baochen, Peng, Chaoge, and Xiang, 2011)

A Survey of Detection Techniques for P2P Botnets

Rawat *et al.* (2018) presented a survey of the evolution, functionalities, modeling and the development life cycle of P2P botnets. Further, the authors investigated the various Peer-to-Peer botnet detection approaches. Zhuang, and Chang (2017) proposed a botnet detection scheme named PeerHunter. The technique used in the work is through Community Behavior Analysis. The authors claimed that PeerHunder has better detection rate for botnets that operate based on peer-to-per architecture when compared to similar studies. Almomani (2016) used a model called Fast-flux hunter for filtering online fast-flux botnets. Similarly, Yan, Zheng, Jiang, Lou and Hou (2015) proposed a system that detects P2P botnet in real time. Mohammed and Selvakumar (2014) reviewed works on peer-to-peer detection techniques. The evaluation work shows that each technique has its own advantages and limitations. The work suggested that two or more detection techniques might be used together, in order to have a robust P2P botnet detection. Ping, Lei, Baber and Cliff (2014) proposed a framework to tackle peer-to-peer botnet attacks by integrating SDN and machine learning to detect and categorize peer-to-peer network traffics. The authors studied Peer-to-Peer botnets systematically by using multiple dimensions such as botnet construction, command and control mechanisms, performance measurements, and mitigation approaches.

David *et al.,* (2013) carried a study that attempts to detect Peer to Peer botnets based on Flow Intervals. The work classified the behavior in the network based on time intervals. The study reported high detection rates but with some limitations to the approach based on the selection of attributes. Bbarthakur, Dahal and Ghose (2013) proposed a comparative analysis of machine-learning based classification of botnet command & control(C&C) traffic for proactive detection of Peer-to-Peer (P2P) botnets. The work compared the performances of Decision Tree (C4.5), Bayesian Network and Linear Support Vector Machines. Wang, Wu, Aslam and Zou (2009) described approaches used by Peer-to-Peer botnets in launching attacks in the cyber scpace. The study then proposed two defence approaches, namely: index poisoning and sybil that can be used for mitigating Peer to Peer botnet attacks. Grizzard *et al.* (2007) presented an overview of peer-to-peer botnets and then presented a case study of a Kademlia-based Trojan.Peacomm bot that has been identified as a popular peer-to-peer botnet. The emphasis of the work is to provide insights on the emergence of a more resilient botnets whose structures are quite different from centralised botnets.

Barford *et al.* (2006) also performed a study that codified malware by comparing four botnet families: Agobot, SDBot, SpyBot and GTBot. The approach used in the study was to exploit the knowledge of basic features of botnet systems so as to improve the host and network-based defensive attempts. The authors provided a good understanding of the details of communication mechanisms in Botnet as it can promote its being taken down easily. Zhao, Traore,Ghorbani, Sayed, Saad and Lu (2012) carried out a study that can identify botnet behavior using machine learning classification techniques. The authors studied the feasibility of detecting botnet activity without having seen a complete network flow by classifying behavior based on time intervals. The two selected Machine Learning algorithms that were used for the experimentation are Bayesian network classifier and a decision tree classifier.

Peer-to-Peer Botnet Detection Evasion Techniques

The basic evasion technique used by P2P botnets is their decentralised architecture. The detection algorithms will find it more difficult to identifying

the C&C server used by the botnet since every bot changes its role (client or server) at intervals.

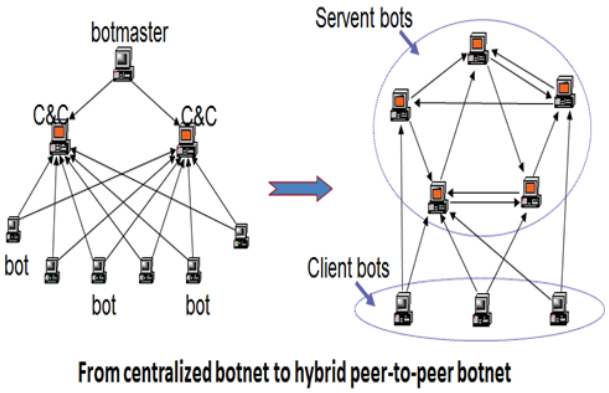

Figure 3: Centralised Botnet Architecture Transforming into P2P Architecture (Zou, 2009)

Past researches have shown that Peer-to-Peer botnets exhibit adversarial tendencies due to the fact that they use different techniques to evade detection (Rawat *et al.,* 2018). Kathrin, Nicholas, Praveen, Michael & Patrick (2009), equally pointed out that there are some effective botnet attacks that have been reported to use adversarial examples against malware detection models. Peer-to-peer botnets particularly used these methods so as to avoid being detected by Intrusion Detection Systems. Botnet attackers have been launching attacks by hiding using the Fast Flux techniques of bonnets. Since the goal of every adversary is to foil the learning algorithm, there is a need for enhanced Machine learning model that can adequately and adaptively guide against peer-to-peer botnets that strive to evade detection. Many learning tasks such as spam filtering and credit card fraud detection face an active adversary that tries to avoid detection (Zhou, Yan, Kantarcioglu and Thuraisingham, 2016).

Internet Relay Chat (IRC) and Hypertext Transfer Protocol (HTTP) based botnets are centralized in nature and usually have a single point of failure unlike Peer to Peer botnet that is decentralised (Barthakur, Dahal & Ghose, 2013). Hybrid Machine Learning models have been identified to, combine completely different, heterogeneous machine learning approaches and can considerably improve quality of reasoning and boost adaptivity of the learning solutions (Castillo, 2007; Corchado, 2010). However, it has been reported that there are massive adversaries that continuously adapt their behaviour so as to hide their nefarious activities and thereby make machine learning detection models ineffective or less effective (Kantarcioglu *et al.,* 2016). Adversarial Machine Learning is the technique that promotes the safe adoption of Machine Learning techniques in adversarial settings. One of the attacks that adversarial malware launch is Poisoning attacks. Poisoning attack is identified by (Yang, Wu, Li and Chen, 2017) as a severe security threat to machine learning algorithms as they have the capability for evading detection models. Lastly, Biggio, Corona, Maiorca, Nelson, Srndic, Laskov and Roli (2017) argued that in security-sensitive applications, the success of machine learning depends on a thorough vetting of their resistance to adversarial data. The work further discussed how Machine Learning algorithms can be evaded by adversarial malware such as peer-to-peer botnets.

Findings and Discussions

The works reviewed have generally shown that botnets operate differently form other categories of malware based on the C&C servers that are used for propagation and launching of attacks. As reported in the literature, this study also found out that the set of emerging botnets that operate on the basis of peer-to-peer architecture have been found to exhibit detection evasion tendencies. Newsome, *et al.* (2006) thus have the opinion that there is an increasing need to device some mechanisms that can adaptively detect and mitigate these adversaries. In building some of the detection models reported, Machine Learning techniques were mostly used. Machine Learning allows learning from large sets of existing data in order to make predictions about new data (Penchikala, 2016). Machine learning is a research approach that allows us to create models from observations called training data for data-driven decision making. In machine learning models, the training process continues until the model achieves a desired level of accuracy on the training data. Decision Tree, Bayesian Network, Support Vector Machines, Random Tree, Neural Network and others have been used to build models that can mitigate botnet attacks. Machine learning uses algorithms that can rapidly analyse, detect, and classify files and behaviour (Sara, 2018), and these algorithms have to be made adaptive for detecting malicious botnets that exhibit detection evasive tendencies. Some of the reviewed works also show that the major detection approach used by researchers is network flow analysis for identifying botnet evidence in the internet space or enterprise networks.

CONCLUSION

This study first of all introduced botnets with particular emphasis on Peer-to-Peer botnets. The work then provided survey on the propagation mechanisms used by the botnet malware. The study equally introduced survey on botnet detection approaches and detection evasive techniques found in literature. This research emphasized that unlike other categories of malware, botnets use Command and Control Server to launch and propagate their attacks and therefore requires adaptable detection approaches. For us to achieve adaptive security models against botnet malware, the suggestion of Zhou, Kantarcioglu and Thuraisinghnam (2016) which claimed that for

all machine learning models that deal with an active adversary, it is important to actively understand the adversary's attack strategy. That is, the learning models for the detection of botnets have to be able to adapt intelligently so as to identify the various detection evasion strategies being used by new variant of botnets. It is believed that identifying such moves will enable security researchers and experts to come up with improved identification and mitigation schemes.

REFERENCES

Alauthaman Mohammad, Aslam Nauman, Zhang Li, Alasem Rafe and Hossain M. A. (2018). A P2P Botnet detection scheme based on decision tree and adaptive multilayer neural networks, *Neural Computing and Applications, 29(11), 991-1004*

Almomani Ammar (2016). Fast-flux hunter: a system for filtering online fast-flux botnet, *Neural Computing & Applications DOI 10.1007/s00521-016-2531-1available at https://www.researchgate.net/publication/306416626*

Banday M.T, Qadri Jameel A. and Shah Nisar A. (2009). *Study of Botnets and The Threats to Internet Security,Association for Information Systems (AIS) Electronic Library,9-24*

Barford P. and Yegneswaran V. (2006). An Inside Look at Botnets, to appear in Series: *Advances in Information Security. Springer, 2006.*

Barthakur, P., Dahal, M., & Kanti Ghose, M. (2013). An Efficient Machine Learning Based Classification Scheme for Detecting Distributed Command & Control Traffic of P2P Botnets. *International Journal of Modern Education and Computer Science, 5(10), 9–18. https://doi.org/10.5815/ijmecs.2013.10.02*

Biggio, B., Corona, I., Maiorca, D., Nelson, B., Srndic, N., Laskov, P and Roli, F. (2017). *Evasion Attacks against Machine Learning at Test Time, 387– 402. https://doi.org/10.1007/978-3-642-40994-3_25*

Bailey Michael, Cooke Evan, Jahanian Farnam, Xu Yunjing & Karir Manish (n.d.). *A Survey of Botnet Technology and Defenses retrieved from https://www.merit.edu/wp-content/uploads/2018/01/Survey_of_Botnet_Technology_and_Defenses.pdf*

Castillo, O., Melin, P., Pedrycz, W. (2007). Hybrid Intelligent Systems: Analysis and Design (Studies in Fuzziness and Soft Computing), Springer, Berlin Heidelber

CERT (2012). Incident Note IN-2002-03 Social Engineering Attacks via IRC and Instant Messaging. *Retrieved from http://www.cert.org/incident_notes/IN-2002-03.html*

Choo, KK. R. (2007). Zombies and Botnets. Trends & Issues in crime and Criminal Justice, 333. *http://www.aic.gov.au/publications/tandi2/tandi333.pdf accessed July 18, 2008.*

Corchado, E., Abraham, A., de Carvalho, A. (2010). Editorial: *Hybrid Intelligent Algorithms and Applications, Information Sciences, 180 (14): 2633–2634*

Feily, Maryam, Shahrestani, Alireza and Ramadass, Sureswaran (2009). A Survey of Botnet and Botnet Detection, *Third International Conference on Emerging Security Information, Systems and Technologies.*

Feily M, Shahrestani & Ramadass S. (2000). A Survey of botnet and botnet Detection, in Proceedings of *IEEE Third International Conference on Emerging Security Information Systems and Technologies, 268-273*

Ferguson, R. (2018). The History of the Botnet. *Retrieved from http://countermeasures.trendmicro.eu/thehistory-of-the-botnet-part-i/ on June 7 2018*

Grizzard Julian B., Sharma V., Nunnery C., Kang B.B. & Dagon D. (2007). Peer-to-Peer Botnets: Overview and Case Study, *Proceedings of the First Conference on First work on Hot Topics in Understanding Botnets retrieved from https://pdfs.semanticscholar.org/2820fe12f286700ca9e7937e4cf3d082fb6d1a23.pdf*

Hyslip, T., & Pittman, J. (2015). A Survey of Botnet Detection Techniques by Command and Control Infrastructure. *Journal of Digital Forensics, Security and Law, 10(1), 7–26. http://doi.org/10.1145/1090191.1080118*

Ianelli N., Hackworth A. (2005). Botnets as a vehicle for online crime, *CERT Request for Comments (RFC) 1700, December 2005.*

Kantarcioglu Murat and Xi Bowei (2016). Adversarial Data Mining: *Big Data Meets Cyber Security DOI: http://dx.doi.org/10.1145/2976749.2976753*

Lei Zhang, Shui Yu, Di Wu, Paul Watters (2011).A Survey on Latest Botnet Attack and Defense, *International Joint Conference of IEEE Trustcom-11/IEEE ICESS-11/FCST-11, 2011*.

Leonard, Justin, Shouhuai, Xu and Sandhu, Ravi (2009). A Framework for Understanding Botnets, Fukuoka :Fukuoka Institute of Technology, *2009 International Workshop on Advances in Information Security*.

Li H. (2012). Research on P2P Botnet Network Behaviour and Modeling

Martinez-Bea, S., Castillo-Perez, S., & Garcia-Alfaro, J. (2013). Real-time Malicious Fast-Flux Detection using DNS and Bot related features. *2013 11th Annual Conference on Privacy, Security and Trust, PST 2013, 369–372. https://doi.org/10.1109/PST.2013.6596093*

Mimoso Michael (2013). Peer-to-Peer Botnets Resilient to Takedown Attempts

Mohammed J.E. and Selvakumar M. (2014). A Review of Peer-to-Peer Botnet Detection Techniques, *Journal of Computer Science 10(1):169-177:*

Muhammad Mahmoud, Manjinder Nir, and Ashraf Matrawy (2013).A Survey on Botnet Architectures, Detection and Defences, *International Journal of Network Security, 0(0), PP.1-19*

Newsome J., Karp B.and Song D. (2006). Thwarting Signature Learning by Training Maliciously, *In Recent advances in Intrusion Detection, LNCS, 81-105, Springer*

Nicholas Lanelli and Aaroon Hackworth (2005). Botnets as a Vehicle for Online Crime, a publication of *CERT Coordination Centre*

Penchikala S. (2016). Big Data Processing with Apache *Spark-Part 4: Spark Machine Learning*

Ping Wang, Lei Wu, Baber Salam & Cliff C. Zou (2014). Analysis of Peer-to-Peer Botnet Attacks and Defences

Rajab M., Zarfoss J., Monrose F., and Terzis A. (2006). A multifaceted approach to understanding the botnet phenomenon, in Proc. 6th ACM SIGCOMM *Conference on Internet Measurement (IMC'06): 41–52*

Rawat Ramesh Singh, Pilli E.S. & Joshi R.C. (2018). Survey of Peer-to-Peer Botnets and Detection Frameworks, *International Journal of Network Security, 20(3):547-557, May 2018 (DOI: 10.6633/ IJNS.201805.20(3).18)*

Sara Baker (2018).A Quick Guide to Machine Learning in Cyber Security

Shannon, C. & Moore, D. (2004). The Spread of the Witty Worm. *Security & Privacy Magazine,2(4): 46-50.*

Shirley Brandon, Lokesh Babu and Chad Mano (2012). Bot Detection Evasion: A Case study on Local-host Alert Correlation Bot Detection Methods, *Networks Security Communications Networks; 5:1277–129*

Ullah, I., Khan, N., and Aboalsamh, H. A. (2013). Survey on botnet : its architecture, detection, prevention and mitigation, (April). https://doi.org/10.1109/ICNSC.2013.6548817

Wang P., Aslam B., and. Zou C. C (2010). Peer-to-Peer Botnets: The Next Generation of Botnet Attacks, *School of Electrical Engineering and Computer Science, University of Central Florida, Orlando, Fla, USA.*

Yan Q., Zheng Y.,Jiang T., Lou W. & Hou T.T. (2015). PeerClean: Unveiling Peer-to-Peer Botnets through Dynamic Group Behaviour Analysis

Yang Chaofei, Wu Qing, Li Hai and Chen Yiran (2017). Generative Poisoning Attack Method Against Neural Networks

Zand A., Vigna G., Yan X., Kruegel C. (2014). Extracting Probable Command and Control Signatures for Detecting Botnets, *Proceedings of the ACM Symposium on Applied Computing (SAC 2014)*

Zhao, D., Traore, I., Ghorbani, A., Sayed, B., Saad, S., & Lu, W. (2012). Peer to Peer Botnet Detection Based on Flow Intervals. *IFIP Advances in Information and Communication Technology, 376 AICT(1), 87–102. https://doi.org/10.1007/978-3-642-30436-1_8*

Zhou Yan, Kantarcioglu and Thuraisinghnam (2016). Adversarial Support Vector Machine Learning

Zhuang, D., & Chang, J. M. (2017).PeerHunter: Detecting Peer-to-Peer Botnets through Community Behavior Analysis. *2017 IEEE Conference on Dependable and Secure Computing, 493–500. http:// doi.org/10.1109/DESEC.2017.8073832*

Zou C.C. (2009). Modeling and Measuring Botnets, Collaborative Research: *CT-ISG, retrieved from http:// www.cs.ucf.edu/~czou/NSF-botnet.htm*