Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 8, 2020

DETECTING BOTNET ATTACK IN INTERNET OF THINGS (IoTs) ENVIRONMENT BY USING MACHINE LEARNING TECHNIQUE: A REVIEW

Samuel Enseriban Belanda[1], Cik Feresa Mohd Foozy[2], Aida Mustapha[3], P. Siva Shamala Palaniapan[4], Zubaile Abdullah[5]

[1,2,3,4,5]**Faculty of Computer Science and Information Technology**
University Tun Hussein Onn Malaysia, Johor Darul Ta'azim
E-mail: hi180031@siswa.uthm.edu.my / samuel.nirv1001@gmail.com / feresa@uthm.edu.my/ aidam@uthm.edu.my

Received: 20.05.2020 ***Revised: 17.06.2020*** ***Accepted: 06.07.2020***

Abstract
Botnet attack are not a new threat in Internet of Things (IoTs) environment. In this globalization world of power information technology where there are less human energy used in daily life, the IoTs has shown it reliability in modern technology world phenomena. As the technology is evolving time to time, the human becomes more interested in exploiting the technology for goods and bad purposes. Example of bad purposed is botnet attack in IoTs environment. The botnet attack nowadays are not only infect the devices massively but also spreading the malicious activities such as Spam, DDoS and more. Hence, in this research, the review of botnet attack in IoTs environment will discuss as well as the method and techniques that used to encounter the attacks too. By spills the beans, the trends of current botnet attacks in IoTs environment will be discuss and follows by reviews of reliable methods for future botnet detection framework.

Keywords--- Botnet, Internet of Things (IoTs), machine learning, feature selection, botnet detection

DOI: http://dx.doi.org/10.31838/jcr.07.08.269

INTRODUCTION

Botnet is a network of connected computer that has been infected with malicious software that has been send and controlled by the 'bot master' without the owner of the computer knowledge(Rezaei, 2018). Botnet is one of the serious setbacks in Internet of Things (IoTs) environment and cyber security.

Botnet attack more than one computers and making them illegally launch and spread the attacks through only one computer (attacker computer) only (Mathur et al., 2018). In the other hand, the botnet is including group pf bots or zombies computer that work together for malicious activities execution in internet world and in Internet of Things (IoTs) environment especially (cybercrime and mobile cloud storage users)(Ray, 2017). Besides that, botnet has becoming a host or medium to broadcasting the attacks on the internet involving DDoS attacks, spamming, and also malicious actions(McDermott et al., 2018).

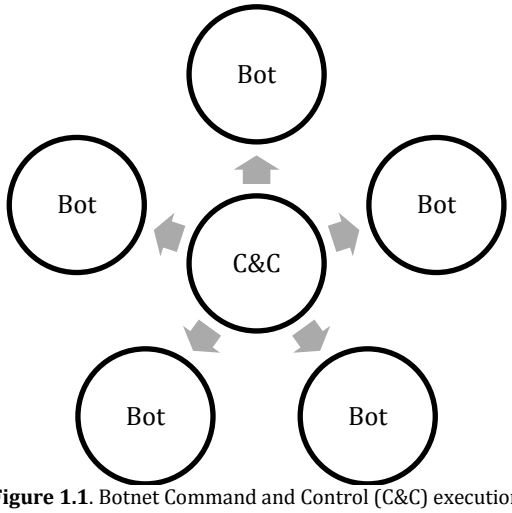

Figure 1.1. Botnet Command and Control (C&C) execution

Figure above shows on how Botnet attacks works. Botnet works via command and control (C&C) algorithm or software that supervised and manage by 'bot master'.

The reason of C&C is to increase the number of bot and manage the operations between the bot and other device in the connection to perform the attacks(Wanting et al., 2019). The attacks of the botnet is carried by the zombies (infected computer which be called as zombie computer)(Lade et al., 2018).

Zombies received the delivery from 'bot master' through C&C execution as well as performing the attacks in the zombies (infected computers) and victim (future-infected computers)(Elzen & Heugten, 2017).

The example attacks that can be executed from the 'bot master' to the zombies are spam attack, worm, virus execution, Distributed-Denial of Services (DDoS), malicious software, Trojan and more(McDermott et al., 2018).

Hence, the main reason of launching the attacks would be to make troublesome in the network of connection between zombies, distributed the spam (annoying spam) and to get information from the zombies (infected computers)(Choi, 2015).

METHODOLOGY

In this section, the research methods and how the studies were conducted that lead to a brief conclusion is discussed and stated. Figure below shows the flow of the review research that lead to the conclusions.

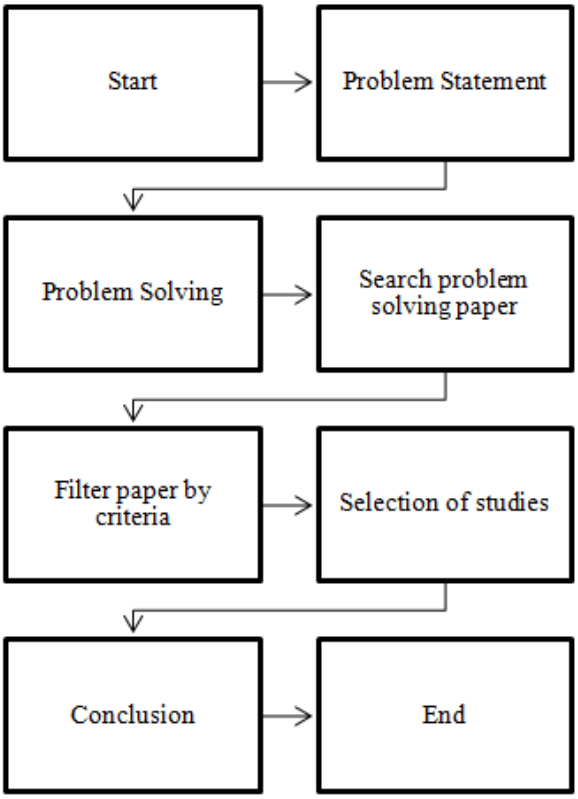

Figure 2.1. Methodology of review research

The review research starts with problem statement. The problem statement for this review research is Botnet attack setback in Internet of Things (IoTs) environment. As been discussed and stated in introduction about the peril of botnet attacks, the problem keeps the research in motivation to be solve by several of techniques. In this advance technology world, the evolvement of the botnet attack also leads to huge impact in security of information technology itself. Besides, the pros and cons of the problem statement is review and revised to be answer and solve in the next step.

The review research continues by problem solving. The problem solving has been solving the problem of revelation had been aided by the help of some search on the internet and some preliminary reading of some papers. There are some papers that used machine learning approach to detect botnet attack as example. For further the review research, the readings proceed as the next steps assist.

The search of problem-solving paper has helped a lot in making this review manuscript to be done. By using "Botnet attack in Internet of Things (IoTs) environment and the approach technique" keywords has found widely and numerous. For example, the paper from Amirhossein Razaei(Rezaei, 2018).

After that, the criteria for considering studies would be based and depends on the three (3) criteria which are the problem statement, technique or methods approach and the paper/journal/manuscripts contributions as well as authors of the paper. As the criteria listed has help to narrowing the research and make the review more precise and specific. The example of criteria searching and studies are shows below.

Table 1. Example of criteria used to for studies and searching

Authors	Problem Statement	Method	Contribution

Besides that, the selection of studies for the future pattern of botnet attack was spam attacks in Internet of Things (IoTs) environment. As the botnet attacks is peril for system where once infected, considered all the network-connected devices also infected in various way off infection(Jerkins, 2017) and (Ghani et al., 2019). Hence, once infected by the botnet attack, the other attack also follows such as DDoS, DoS, identity theft, spam and more(H. Singh & Bijalwan, 2016).

At the end of the studies, the conclusion be made. As the spam in Internet of Things (IoTs) environment are effect by the penetration of botnet attack into the system through the network connection. Furthermore, the further understanding on this review research will be discuss on the next section. Hence, the details about the attacks and the future works would be as follows sections.

LITERATURE REVIEW

The key objectives of this research are to identify the best available botnet detection techniques, and present different existing models for botnet review detection and available parameters to analyse those models accordingly. Hence, in this section, the review of the botnet attack in Internet of Things (IoTs) environment will be discuss. As the table below shows the summary of related paper or research that has been conducted by researchers around the world to identify and counter the botnet attack in IoTs environment.

Table 2. Current research on botnet attack in Internet of Things (IoTs)

Authors	Problem	Method	Contribution
(Ghomeshi et al., 2018)	In non-stationary environments of IoTs, the data/class of classification of machine learning technique in classification has been evolved over the time accordingly. This phenomenon was called *"concept drift"*.	Ensemble Dynamics in Non-stationary Data Stream Classification was proposed by the researcher to overcome the setback.	The *concept drift* of Internet of Things environment has been solved by proposing the ensembles dynamics in Non-Stationary Data Stream Classification where the classification will be either effectively classified the botnet or not and is it malicious or not malicious.
(Lade et al., 2018)	Difficulties in detecting botnet as the command and control (C&C) application are executed.	Signature based detection, firewall IP blocking and anomaly based detection technique are proposed	Discussed and pictures the botnet attacks along with its consequences. Hence, three (3) different techniques of detection botnet are proposed.

(Khamis et al., 2014)	Web-based attack that launched by attacker has hit the chart of web-based chart. There will be more than one ways to counter the attack such as detection and prevention.	Create a malicious page detection framework by using supervised machine learning techniques which are support vector machine (SVM), K-Nearest Neighbour (KNN), and Artificial Neural Network (ANN)	A framework for identifying a malicious page is proposed by using supervised machine learning techniques which are Support Vector Machine (SVM), K-Nearest Neighbour (KNN) and Artificial Neural Network (ANN).
(H. Singh & Bijalwan, 2016)	To specified the botnet attack through the network and the system need to be cleared such as how the botnet working, effect of botnet attacks and the way of detection and prevention of botnet need to be known for better botnet detection framework.	Implementing honey net in the network for penetration testing purpose before the packet of data entered the gateway. Passive traffic monitoring is implemented for detection purposed. The detection will include signature based detection, anomaly based detection, DNS based detection, and mining based detection	The studies and analysis of botnet attacks, malware categories, botnet formation and workings, differences of botnet and detection of botnet are discuss in the findings for a better detection in future botnet detection framework.
(H. Singh & Bijalwan, 2017)	Botnet attack has been increasing in internet environment as the evolvement of internet technology is rapid yearly.	Implement the botnet detection framework systematically and effectively by present the analysis approaches in botnet detection	Popular and most common botnet detection techniques are present in analysis way which are host based, honeynet and network based detection technique. For proposed analysis technique of botnet detection, the researcher stated that there are three major steps which are pre-identification, identification and detection.
(Blessing et al., 2018)	The evolving of botnet attack is currently an issues to be handle as soon as possible as the spread of the attack are massive and fast where one device infected then, the other devices that connected to the same network will be infected as well.	The architectural, classification and characterization representation are present and analysed as review is made by the researcher.	The details review of overall architecture and characterization of botnet attack was clearly be present as the centralized and decentralized botnet architecture are discuss accordingly. Hence, the botnet detection techniques to counter the attack has been shown by the researcher as machine learning based are present as long as other based technique are well explain.

As the table shown the past researchers has been proven that the botnet attack is massive as the evolving of the Command and Control (C&C) application for attack executions. With the help of artificial intelligent or specifically machine learning techniques was approaches, the botnet attack can be countermeasure and to be solved as well by proposed the detection framework (McDermottet al., 2018). In other words, the botnet attack are consequently pushing the attacks to all of the infected devices where the data or information that has been send and received through the network transaction will be high in volume where the data and information can be only measure and handle by using machine learning techniques(Nomm& Bahsi, 2019).

According to the Prokofiev et al., 2018 (Prokofiev et al., 2018), the botnet in Internet of Things (IoTs) environment are evolving and changing its game play where the botnet attacks is carrying other triggering malicious attacks such as spam attack, DDoS and more. In conjunction of that, the next section will discuss the future pattern of botnet attacks in IoTs environments.

BOTNET ATTACK PATTERN IN FUTURE

In this section the future pattern of botnet attack will be discuss. The future botnet attacks are actually current pattern of botnet attacks that has been virally distributed it popular-ness where the attacks are not only control the infected devices by using Command and Control (C&C) application but also distributed malicious software and activities such as Spam distribution and DDoS attacks(Pu et al., 2019). Table below shows the past research about the malicious activities in botnet attacks based in Internet of Things (IoTs) environment.

Table 3. Current botnet attack pattern review

Authors	Problem Statements	Methods and Contributions
(Makkar & Kumar, 2019)	The existing techniques in spam injection through the search engine in the IoTs environment should be able to prevent spam in IoTs search engines itself. But, the existing techniques was unsatisfied the detection of spam in search engine on IoTs's search engine.	To overcome this problem, an intelligent cognitive spammer framework was proposed, or the other name was "Cognitive spammer". The framework works to eliminate the spam pages during the web page rank score calculation by search engines. Besides, the framework help by PageRank to prevent link spam automatically.
(Rezaei, 2018)	Identify and detecting the Botnet attack in Internet of Things (IoTs)The Botnet is normally used to send spam, steal data, carry out DDoS attack, it also allows the	Review recent studies has been done in the matter of detecting Botnet by using supervised learning and unsupervised learning techniques with aim of finding advantages and disadvantages of each also

	attacker to access the devices and their connections	to discover which one is more appropriate for identifying Botnet during communication between IoTs and cloud
(A. Singh & Batra, 2018)	In IoTs, a large number of objects need to be connect in large number as such as devices to devices notification which acquired the communication mass through the internet itself. Hence, a social approach is one of the mass communication medium for the communication like Twitter, Facebook, Instagram, etc. By the meantime, the dynamic discovery of services and information have to be simplified within the social network of IoTs domain. In conjunction of that, the daunting task will requires lot of technical insight which cause when massive data flows continuously and larger number of attributes are associated with it such as detecting spam in social media through the internet domain sniffing and detecting.	Therefore, the researcher has proposed a way in order to overcome the problem. A semi-supervised technique for spam detection in Twitter by employing ensemble based framework comprising of four classifiers was proposed.
(Kambourakis et al., 2017)	The most popular attacks in IoTs and other technology that using blockchain algorithm/paradigm is Mirai. In this Kambouris et al., 2017 paper, a massive attack of DDoS by launching the Mirai family of malware increasing the volume and diversity to assemble the botnets. The botnets is assemble to spread DDoS, spam and advertisement fraud in IoTs environment.	A comprehensive review of botnet attacks nature has been made. The review technically discussed the reasons of Mirai malware focus on successful-attack on IoTs devices by provide the details on the internal workings of the Mirai malware and at conclusion, the researcher has explain the possible strategies according to their hypothesis and review for defending the IoTs devices against the Mirai malware.
(Li et al., 2019)	In order to protect the IoTs system from spam email, machine learning is approaches to mitigate the spam classification problem. Hence, the machine learning technique consume much time and expensive at the same time, which would affect the effectiveness of the spam classification framework.	In order to overcome the problem, the researcher's team proposed a design of multi-view based in email classification of spam detection for IoTs systems using machine learning techniques which was specifically a semi-supervised learning.
(Taheri et al., 2018)	In Internet of Things (IoTs) environment, the botnet attack are famous as it can contribute other massive attacks on IoTs environment, as it can shoots two birds by using a stone phenomenon. The examples of attacks distributions from botnet attack would be (DDoS), SPAM, identity theft, phishing, and espionage. As the time goes by, the techniques of botnet detection has out of affection as the evolving of the botnet pattern and phenomenon.	Hence, the researchers has proposed a botnet detection using deep learning-based engine to overcome the problem. The technique will technically transform the normal and botnet network traffic data into image. Then, after the image was created which transform from the network traffic data, the convolutional neural network, named DenseNet will do the work with or without considering the transfer learning.
(Paavolainen et al., 2019)	In IoTs environment, the smart contract have no fairness and guarantees eventually. The smart contract is also one of the transactions in the Ethereum network which mainly aim as IoTs handshake interchange for trust each device to make transaction. Hence, there are possibility of spam attack to sufficient the cryptocurrency to statistically obvious in delay on transaction send and received by the Ethereum network.	The researchers has proposed a probability value on the costs as well as effects of spam attacks in Ethereum network based on an analysis of transaction history.
(Meidan et al., 2018)	In the evolving of IoTs technology, the number of botnet attack in IoTs	Meidan et al., 2018 has proposed an evaluation of novel network-based detection method. The

	senvironment is the increasing which could lead to massive DDoS, spam and Identity theft attack. To overcome the problem, various ways of detecting the attack is proposed. Besides, as the detection of botnet attack proposed, the differentiation also been made.	method extracts the behaviours of the network by using deep autoencoders for the detection of anomalous network traffic penetrating the IoTs devices.

The table explain that the past researcher has mentioned that the botnet attack is not only infect the devices and manipulated the devices accordingly by using Command and Control (C&C) application but also spreading the malicious activities such as Spam distributions and DDoS distribution. In the table above mention a few about the spam trends in the botnet attacks. The spam might be in notification spam, Voice over Internet Protocol (VoIP) and Short Message Services (SMS) Spam as well.

CONCLUSION

By demanding the bright future of modern information technology phenomena, the increase of internet-connected device will put the high risk of botnet attacks widely. The problem of botnet attack arise as the level of information security of the internet-connected devices are remains low. That's the main reason of botnet attacks are stepping stone for performing massive and actively DDoS and Spam attacks employed by cybercriminals around the globe.

To essentially defence against IoTs botnets, few techniques to detect botnet is a must and effectively essential. In this research, the techniques used by past researchers are clearly elaborated and summaries for better references in future works of botnet detection framework.

ACKNOWLEDGEMENT

Endless thanks for the supporter for this research which was supported by the Ministry of Education Malaysia under the Fundamental Research Grant Scheme (FRGS)Vot No. FRGS/1/2018/ICT04/UTHM/03/4 and partially sponsored by University Tun Hussein Onn Malaysia. Thanks to colleagues from Universiti Tun Hussein Onn Malaysia (UTHM) and Faculty of Computer Science and Information Technology (FSKTM), UTHM who provided insight and expertise that greatly assisted the research as they agree with all of the interpretations and conclusions of this paper .Huge thanks to Dr CikFeresaMohdFoozy and Dr. Aida Mustapha for assistance with machine learning technique and for comments that greatly improved the manuscript.

REFERENCES

1. Blessing Nwamaka, I., & Raphael Okonkwo, O. (2018). Analysis of Botnet Classification and Detection Techniques: A review. *JETIR 2018*, *5*(10), 2015–2017.
2. Choi, T. (2015). System and method for detectng malicious mail from spam zombies. *Google Patents*, (US 9,083,556 B2). Retrieved from https://patents.google.com/patent/US9083556B2/en
3. Elzen, I. van der, & Heugten, J. van. (2017). Mirai Detailed Analysis. *University of Amsterdam*, 25. Retrieved from http://www.delaat.net/rp/2016-2017/p59/report.pdf
4. Ghani, A.B.A., Mahat, N.I., Hussain, A., Mokhtar, S.S.M. (2019). Water Sustainability In Campus: A Framework In Optimizing Social Cost. International Journal of Recent Technology and Engineering, 8 (2 Special Issue 2), pp. 183-186.
5. Ghomeshi, H., Gaber, M. M., & Kovalchuk, Y. (2018). Ensemble Dynamics in Non-stationary Data Stream Classification. In *Springer* (pp. 123–153). https://doi.org/10.1007/978-3-319-89803-2_6
6. Jerkins, J. A. (2017). Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code. *2017 IEEE 7th Annual Computing and Communication Workshop and Conference, CCWC 2017*. https://doi.org/10.1109/CCWC.2017.7868464
7. Kambourakis, G., Kolias, C., & Stavrou, A. (2017). The Mirai botnet and the IoT Zombie Armies. *Proceedings - IEEE Military Communications Conference MILCOM*, *2017-Octob*, 267–272. https://doi.org/10.1109/MILCOM.2017.8170867
8. Khamis, A., Baharudin, B., & Jung, L. (2014). Characterizing A Malicious Web Page. *Australian Journal of Basic and Applied Sciences*, *7*(11), 69–76.
9. Lade, M., Bakal, J. W., & Jayamalini, K. (2018). Different Techniques to Detect Botnet. *INTERNATIONAL JOURNAL ON RECENT AND INNOVATION TRENDS IN COMPUTING AND COMMUNICATION*, *6*(2), 61–64.
10. Li, Wanting, Jin, J., & Lee, J.-H. (2019). Analysis of Botnet Domain Names for IoT Cybersecurity. *IEEE Access*, *7*, 94658–94665. https://doi.org/10.1109/access.2019.2927355
11. Li, Wenjuan, Meng, W., Tan, Z., & Xiang, Y. (2019). Design of multi-view based email classification for IoT systems via semi-supervised learning. *Journal of Network and Computer Applications*, *128*, 56–63. https://doi.org/10.1016/j.jnca.2018.12.002
12. Makkar, A., & Kumar, N. (2019). Cognitive spammer: A Framework for PageRank analysis with Split by Over-sampling and Train by Under-fitting. *Future Generation Computer Systems*, *90*, 381–404. https://doi.org/10.1016/j.future.2018.07.046
13. Mathur, L., Raheja, M., & Ahlawat, P. (2018). Botnet Detection via mining of network traffic flow. *Procedia Computer Science*, *132*, 1668–1677. https://doi.org/10.1016/j.procs.2018.05.137
14. McDermott, C. D., Majdani, F., & Petrovski, A. V. (2018). Botnet Detection in the Internet of Things using Deep Learning Approaches. *Proceedings of the International Joint Conference on Neural Networks*, *2018-July*. https://doi.org/10.1109/IJCNN.2018.8489489
15. McDermott, C. D., Petrovski, A. V., & Majdani, F. (2018). Towards situational awareness of botnet activity in the internet of things. *2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2018*. https://doi.org/10.1109/CyberSA.2018.8551408
16. Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-BaIoT-Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, *17*(3), 12–22. https://doi.org/10.1109/MPRV.2018.03367731
17. Nomm, S., & Bahsi, H. (2019). Unsupervised Anomaly Based Botnet Detection in IoT Networks. *Proceedings - 17th IEEE International Conference on Machine Learning and Applications, ICMLA 2018*. https://doi.org/10.1109/ICMLA.2018.00171
18. Paavolainen, S., Elo, T., & Nikander, P. (2019). Risks from Spam Attacks on Blockchains for Intemet-of-Things Devices. *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2018*, 314–320. https://doi.org/10.1109/IEMCON.2018.8614837
19. Prokofiev, A. O., Smirnova, Y. S., & Surov, V. A. (2018). A method to detect Internet of Things botnets. *Proceedings of*

the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2018, *2018-Janua*, 105–108. https://doi.org/10.1109/EIConRus.2018.8317041

20. Pu, C. (2019). Spam DIS Attack Against Routing Protocol in the Internet of Things. *2019 International Conference on Computing, Networking and Communications, ICNC 2019*, 73–77. https://doi.org/10.1109/ICCNC.2019.8685628
21. Ray, P. P. (2017). A survey of IoT cloud platforms. *Future Computing and Informatics Journal*, *1*(1–2), 35–46. https://doi.org/10.1016/j.fcij.2017.02.001
22. Rezaei, A. (2018). Identifying Botnet on IoT and Cloud by Using Machine Learning Techniques. *Open International Journal of Informatics (OIJI)*. Retrieved from http://apps.razak.utm.my/ojs/index.php/oiji/article/download/63/40
23. Singh, A., & Batra, S. (2018). Ensemble based spam detection in social IoT using probabilistic data structures. *Future Generation Computer Systems*, *81*, 359–371. https://doi.org/10.1016/j.future.2017.09.072
24. Singh, H., & Bijalwan, A. (2016). A survey on Malware, Botnets and their detection. *International Journal of Advanced Engineering Research and Science (IJAERS)*, *3*(3), 85–90.
25. Singh, H., & Bijalwan, A. (2017). A Framework on botnet detection and forensics. *Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering*, *10*, 93–101. https://doi.org/10.15439/2017r28
26. Taheri, S., Salem, M., & Yuan, J.-S. (2018). Leveraging Image Representation of Network Traffic Data and Transfer Learning in Botnet Detection. *Big Data and Cognitive Computing*, *2*(4), 37. https://doi.org/10.3390/bdcc2040037