INTERNATIONAL JOURNAL
OF TECHO-ENGINEERING

ISSN : 2057-5688

A SURVEY –DETECTION OF MALICIOUS SOCIAL BOTS IN SOCIAL NETWORK

[1]EEDUNURI UMA MAHESHWARI, [2]M.UDAY KUMAR

[1] M.Tech Scholar ,[2]Associate Professor, Dept of CSE,

JNTUH UNIVERSITY COLLEGE OF ENGINEERING, JAGTIAL, T.S, INDIA.

Abstract: Social bots, a new generation in bots, make use OSNs as command and controlling (C&C) channels. Malicious social bots have been misused to launch large-scale spam attacks, promote low-cap stocks and manipulate users' influence online. Recent research has focused on either general security issues in social networks or coarse-grained categorizations to assist detection. This survey seeks to provide a comprehensive analysis through a social networking perspective. To do this, we first divide social bot attacks into different stages. Then, we provide an overview about different types. Next, we create a refined taxonomy showing how different techniques within the same category are related or distinct from one another. We then discuss each method's strengths and shortcomings. After reviewing the data, we summarize empirical research results and review the existing datasets. We also highlight the weaknesses of existing detection strategies and recommend future directions. Our research should assist OSN administrators and researchers in understanding the destructive potential of social bots. It will also help them to develop new defensive strategies..

.

Keywords: Security,Online social networks, Social bots, Taxonomy, Malicious behavior.

1 . INTRODUCTION:

Botnets are networks of bots or zombies that have been infected with bots and then controlled by an attacker (botmaster). This is to carry out malicious activities. Botmaster can take control of the server to initiate cyberattacks such as spam, phishing and click fraud. This is one of the most dangerous security threats facing the Internet. Due to the constant development of botnets and the security risks associated with them, it is difficult for academic and industrial researchers to accurately identify and detect botnets. First, botnets' C&C mechanisms exhibit intelligent and diverse characteristics. Botnets have been able to take advantage of public resources like 5G, Internet of Things and smart terminals. Botnets make use of technologies like zero-day vulnerabilities and P2P networks. Phishing, fast flux, anonymous networks and bitcoin networks are some of the ways they spread and can be used to spread. Second, botnets are faster to spread than conventional network security threats. They have more infection channels, are easier to conceal, have more technical content, and can be more destructive than traditional ones. Botnets, which are often in a silent state, maintain the connection state via C&C channels. They do not attack or intrude, but they can also be used to maintain it. Most intrusion detection systems are unable to detect botnets.

It has been a rapid development in deep learning theory. There have been significant advances in related theoretical research [7, 8], and in practical applications [8, 9]. Deep learning methods are capable of solving common zombies. Researchers have turned to multiclassification task recognition's low accuracy rate and the complexity in feature engineering in the network detection technology as research hotspots. The unique features of blockchain technology, including decentralization, anticensorship. and concealment, along with smart contracts, signatures, incentives mechanisms, create a new paradigm for building botnets. The community mining algorithm within the complex network discipline offers new ideas to conduct behavior-based analysis of botnets. Swarm intelligence algorithms are among the most recent methods for botnet analysis. These include MTD, SDN and integrated methods..

2. PREVIOUS SURVEYS

Many surveys have been done on botnet detection technology in the recent past. They are examined in this section. The IoT network-based botnet detection technologies can also be classified as host-based and system-based in [9]. Network-based detection further sub-divides into signature-based DNS-based traffic-based anomaly-based and mining based methods. This review is only a partial overview of IoT botnets. [10] contains a complete statistical analysis on IoT attack literature from the recent years. The review provides a detailed analysis of IoT attack literature in recent years. However, the review does not provide a detailed description of the detection technology or analyze the methods.

There are five main categories of DNS-based botnet identification technologies: flow-based or anomaly-based, flux based, DGA based, DGA based, and bot infected-based. These attributes are essential for a smart DNS,-based botnet identification system. However, the survey provided no context for the botnet's construction process. [12] - A complete botnet detection analysis is available.

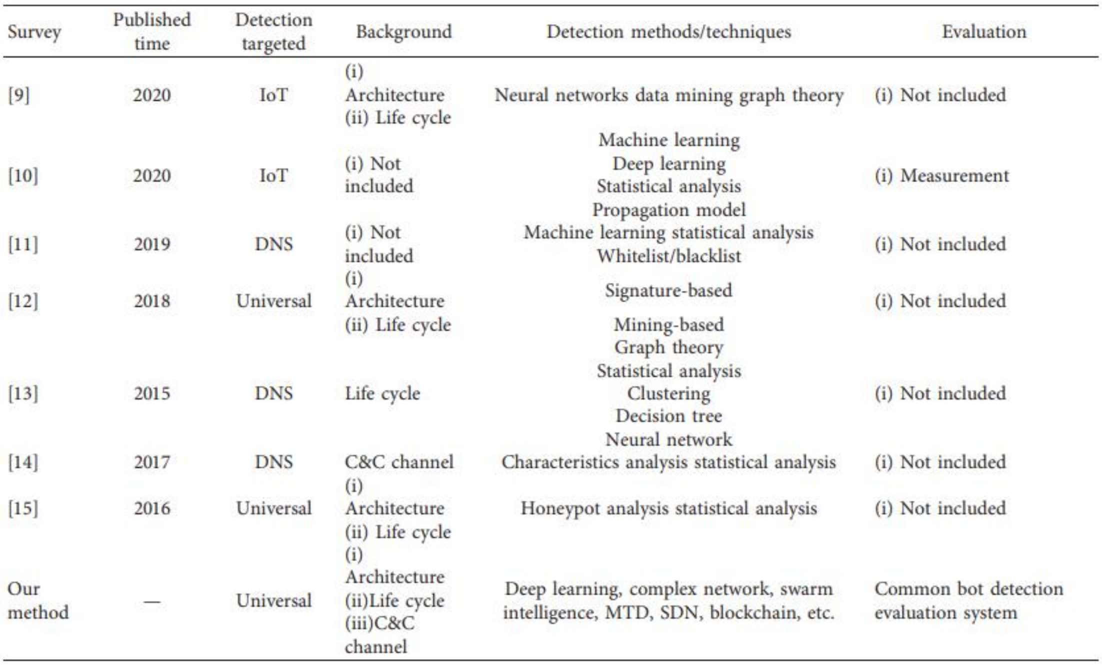
This survey separates botnet detection techniques in four classes: anomaly, signature, DNS, mining, and DNS. Unfortunately, the summary is not comprehensive enough to include the most recent technology. Botnet detection technologies based off DNS traffic analysis are classified in [13] into two categories: honeypot and IDS. It introduces passive technologies including graph theory. Although the literature is extensive, they are not yet evaluated. [14] discusses detection and mitigation techniques for DNS-based malware botnets. This survey introduces Fast-Flux, DGA and DGA botnet identification technology. Additionally, the dimensions of this survey are not very large and there is no evaluation.

.

3. BACKGROUND

This section provides an overview of recent developments in botnet construction based on a deep understanding of the working mechanisms and behavior characteristics botnets.

Table 1: Comparison with other surveys.



Survey	Published time	Detection targeted	Background	Detection methods/techniques	Evaluation
[9]	2020	IoT	(i) Architecture (ii) Life cycle	Neural networks data mining graph theory	(i) Not included
[10]	2020	IoT	(i) Not included	Machine learning Deep learning Statistical analysis Propagation model	(i) Measurement
[11]	2019	DNS	(i) Not included	Machine learning statistical analysis Whitelist/blacklist	(i) Not included
[12]	2018	Universal	(i) Architecture (ii) Life cycle	Signature-based	(i) Not included
[13]	2015	DNS	Life cycle	Mining-based Graph theory Statistical analysis Clustering Decision tree Neural network	(i) Not included
[14]	2017	DNS	C&C channel	Characteristics analysis statistical analysis	(i) Not included
[15]	2016	Universal	(i) Architecture (ii) Life cycle	Honeypot analysis statistical analysis	(i) Not included
Our method	—	Universal	(i) Architecture (ii)Life cycle (iii)C&C channel	Deep learning, complex network, swarm intelligence, MTD, SDN, blockchain, etc.	Common bot detection evaluation system

4. CLASSIFICATION

Conventional detection methods are no longer suitable for new botnet detection. Many botnet detection strategies have been developed by the industry to gain a deeper understanding of the botnet's behavior and working mechanism. This section lists the top technologies for botnet identification into three categories, based on honeypot analyses, communication signatures, or abnormal behavior[16,17]. We concentrate on the application deep learning and complex networks, swarm intelligent, MTD/SDN, blockchain, as well other cutting-edge technologies in Botnet detection. Different botnet detection technologies classification standards exist, and there are multidimensional classification methods.

5. METHODS

5.1. Based on Honeypot Analysis. Based on the honeypot

analysis and detection method. Many malicious codes samples can also be obtained via honeypot capture, i.e. botnet binary data files. In a controlled environment monitoring and analysis of these files can be done and bots and malicious behavior can be found. It is an active detection activity[18].

5.2. Based on Communication Signature.

The communication signature detection method is a well-used defense method. It detects bot activities based in predefined patterns and signatures obtained from well-known bots. These methods include regular expressions as well whitelists (or blacklists) and Ngram models. Snort is able to detect botnet activity quickly and accurately by configuring feature matching rules ahead of time. Communication signature-based detection is best for botnets having definite features. This method helps to better understand botnet communication and possible vulnerabilities. Robots cannot be used to bypass signature-based detection. They can also use code obfuscation technologies, but this does not allow them to detect botnets containing unknown features[19]. The method must continuously update and maintain the signature knowledge, increasing the cost of detection

5.3. Based on Abnormal Behavior. Botnet detection research is dominated by anomaly-based detection. This idea is based upon host behavior and network traffic abnormalities. It includes traffic on abnormal ports and traffic on high latency networks[20]. It is possible to detect a deviation from the normal behavior or a similarity with bots' behavior.

6. CONCLUSION

This survey presents the new botnet construction method, reviews the most recent technologies in botnet detection and compares key technologies that are based on anomaly. This paper proposes an evaluation system to evaluate all detection methods. There are always new botnets, so research in this area will continue to be a priority.

This survey is crucial for security personnel who need to analyze and defend botnets. It may also help researchers to develop better tools and techniques to mitigate the threat from botnets.

Conflicts of Interest The authors declare that they have no conflicts of interest..

7 . REFERENCES:

[1] B. Fang, X. Cui, and W. Wang, "Survey of botnets," Journal of Computer Research and Development, vol. 48, no. 8, pp. 1315–1331, 2011, (in Chinese).

[2] G. Vormayr, T. Zseby, and J. Fabini, "Botnet communication patterns," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2768–2796, 2017.

[3] A. Karim, R. B. Salleh, M. Shiraz et al., "Botnet detection techniques: review, future trends, and issues," Journal of Zhejiang University Science, vol. 15, no. 11, pp. 943–983, 2014.

[4] M. Casenove and A. Miraglia, "Botnet over tor: the illusion of hiding," in Proceedings of the 6th international conference on cyber conflict, CyCon 2014, tallinn,Estonia, pp. 273–282, Tallinn, Estoni, June 2014.

[5] T. Curran and D. Geist, "Using the bitcoin blockchain as a botnet resilience mechanism," 2016, https://www.os3.nl/ media/2016-2017/courses/ot/dana/tom.pdf.

[6] A. Kurt, E. Erdin, M. Cebe, K. Akkaya, and A. S. Uluagac, "LNBot: a covert hybrid botnet on bitcoin lightning network for fun and profit," in Computer Security – ESORICS 2020. ESORICS 2020, L. Chen, N. Li, K. Liang, and S. Schneider, Eds., Springer, Berlin, Germany, 2020.

[7] P. F. Cui, Y. Qiu, and R. Sun, "Research on image recognition technology for the network content security," Netinfo Security, vol. 9, pp. 154–157, 2015.

[8] K. S. Q. Gul, J. Z. Yin, L. M. Pan et al., “Research on the algorithm of named entity recognition based on deep neural network,” Netinfo Security, vol. 10, pp. 29–35, 2017.

[9] S. Dange and M. Chatterjee, “IoT botnet: the largest threat to the IoT network,” in Advances in Intelligent Systems and Computing, L. Jain, G. Tsihrintzis, V. Balas, and D. Sharma, Eds., Springer, Berlin, Germany, 2020.

[10] I. Ali, A. I. A. Ahmed, A. Almogren et al., “Systematic literature review on IoT-based botnet attack,” IEEE Access, vol. 8, pp. 212220–212232, 2020.

[11] M. Singh, M. Singh, and S. Kaur, “Issues and challenges in DNS based botnet detection: a survey,” Computers & Security, vol. 86, pp. 28–52, 2019.

[12] M. Sandip Sonawane, “A survey of botnet and botnet detection methods,” Nternational Journal of Engineering Research & Technology (IJERT), ISSN, vol. 7, no. 12, 2018.

[13] K. Alieyan, A. Almomani, A. Manasrah, and M. M. Kadhum, “A survey of botnet detection based on DNS,” Neural Computing and Applications, vol. 28, no. 7, pp. 1541–1558, 2017.

[14] X. Li, J. Wang, and X. Zhang, “Botnet detection technology based on DNS,” Future Internet, vol. 9, no. 4, p. 55, 2017.

[15] K. Li, B. Fang, X. Cui, and Q. Liu, “Study of botnets trends,” Computer Research and Development, vol. 53, no. 10, pp. 2189–2206, 2016.

[16] C. Y. Liu, C. H. Peng, and I. C. Lin, “A survey of botnet architecture and batnet detection techniques,” International Journal of Network Security, vol. 16, no. 2, pp. 81–89, 2014.

[17] R. A. Rodr´ıguez-Gomez, G. Maci ´ a-Fern ´ andez, and P. Garc ´ ´ıaTeodoro, “Survey and taxonomy of botnet research through life-cycle,” ACM Computing Surveys, vol. 45, no. 4, pp. 1–33, 2013.

[18] K. Li, Research on Botnet Countermeasures Based on Behavioral Analysis, Beijing University of Posts and Telecommunications, Beijing, China, 2017. [19] J.

Canavan, “*e evolution of malicious IRC bots,” in Proceedings of the Virus Bulletin Conference, pp. 104–114, Dublin, Ireland, October 2005.

[20] R. Fielding, J. Gettys, J. Mogul et al., “Hypertext Transfer Protocol – HTTP/1.1,” RFC 2616, 1999.

[21] J. Stewart. (2004, Mar.) Phatbot Trojan Analysis. SecureWorks. http://web.archive.org/web/20080917193007/http://www.secureworks.com/research/threats/phatbot/.

[22] R. Sharpe, “Just what Is SMB,” V1.2, Oct. 2002.

[23] Higgins K. J.. Smartphone weather app builds a mobile botnet [EB/OL]. (2010-03-05) [2016-06-14].-http://www. darkreading.com/risk/smartphone-weather-app-builds-amobile-botnet/d/d-id/1133138” http://http//www. darkreading,%20com/risk/smartphone-weather-app-buildsa-mobile-botnet/d/d-id/1133138%20.

[24] S. Dange and M. Chatterjee, “IoT botnet: the largest threat to the iot network,” in Data Communication and Networks. Advances in Intelligent Systems and ComputingSpringer, Berlin, Germany, 2020.

[25] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the iot: mirai and other botnets,” CyberTrust by IEEE Computer Society, vol. 43, 2017.