International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

Effect of Social Media Botnets and their Detection Techniques

Amit Jain, Anand Kumar Shukla, Raju Kumar

Abstract: ***The Online Social Network (ONS) or Social Media have become most popular platform for millions of users for their activities and at the same time it has become favorite place for cyber criminals for their illegal activities, generally known as social botnets, which uses different techniques to spread their information on social media like facebook, twitter, renren, linkedin etc. Several researchers have tried to detect several social botnets with different detection techniques. To avoid the detection, social botnets are now using advanced command & control (C&C) communication channels like hash tags, fraud click, friend requests, images, videos etc.***

Image Steganography techniques are now widely being used to carry out attacks. In this paper, the primary discussion is related to effects of social media botnets along with the different techniques for botnet detection. It also, explores the use of machine learning mechanism, thereby detecting the intrusions in stegano images. Thus, an effort has been made to localize the factors that have a major role in social intervention as a whole.

Keywords: Botnets, Social Media, Steganography

I. INTRODUCTION

Primarily, the social networks are web-based services connecting millions of people across the globe which provides a platform so that people can interact and communicate with each other. People have social media accounts and use it to interact with each other and share their messages, pictures, videos, events. Because of its rapid growth, it is used for commercial, political and religious purposes also. The social network as a coin has two faces-one useful and other darker. But it has been a platform for various malicious users as well, like spreading of fake news, stealing confidential information, spamming, terrorist activities, phishing etc.

The biggest threat nowadays to social network is Botnet. This botnet in real sense is a network of negotiated PCs. Due to malicious code these computers are infected and are remotely controlled through common command and control channel or (C&C). This channel is called as botmaster. Not only can these botnets be constructed using existing popular applications such as HTTP or IRC but can also be created by using unknown or some creative kind of applications.

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
Dr. Amit Jain*, Associate Professor, University Institute of Computing, Mohali, India. Email: amit_jainci@yahoo.com
Dr. Anand Kumar Shukla, Associate Professor, University Institute of Computing, Mohali, India. Email: amit_jainci@yahoo.com
Dr. Raju Kumar, Associate Professor, University Institute of Computing, Mohali, India. Email: rajuk12@gmail.com

That is why detecting botnets is a problem with challenges. They are being used for DDoS attacks, spamming, phishing attacks, malicious link spreading and other kinds of unlawful activities through social networks as their main medium.

One of the first IRC based bot discovered in 1993 [16,23] and an ONS based bot which was discovered on Aug, 3rd 2008 targeted social networking sites like Facebook and Twitter etc. They perform various activities which are malicious in nature like spamming, user information stealing, search hijacking etc. Similarly, another kind of bot called as Naz was indentified on twitter in 2009[1, 23] and Poney bot found in Dec, 2013 have extracted around 2 million plus passwords from social network sites like Facebook and Twitter [2, 23]. The main platform being used by these bots is social media and their detection is very important as they are responsible for various kinds of attacks like [5, 6], fake news and malicious information spreading [7, 8], stock market manipulations and intelligence collection [23, 24] etc.

There are several loopholes in the current detection methods. Because the technology keeps on getting sophisticated, botnets accordingly are also using new methods for the intrusion purpose so as to avoid the process of their detection. Because these bots are using various new ways like fraud clicks, hash tags, friend requests and steganography etc. One can say that the detection of these botnets is very challenging. The detection process of these social botnets is exponentially increasing and is continuously evolving so as to evade the latest detection mechanisms.

II. PROBLEM DEFINITION

Currently, we are in an era where one can't imagine social interaction without Online Social Networks (OSN) as billions of people have social media accounts to interact with each other or to gather or spread information at any time. Also, one can create social content and share their pictures, videos and events and these features render them not only for private use but also for commercial, political and religious purposes as well. As has been mentioned earlier thee social botnets pose the biggest threat to OSN sites. Cyber criminals utilize social botnets to accumulate intelligence, extend influence and harmful information.

Currently, there are numerous kinds of bot attacks like hash tag hijacking, where the motive is to target some groups or organizations by recognizing some specific hash tags. Here, bots keep on spreading spams, attaching some abusive and unrelated links, discuss totally unrelated stuff that appears in group and feeds with a focus to attack that very group [24]. Now a days, attack on hash tag based tweets is also happening, so as to seek attentions, posting abusive and malicious content through trending hash tags.

To detect this hash tag hijacking process, in one of the study a tool called HashJacker is proposed which detect and analyze hijacking of these hash tag tweets [26].

It performs a dictionary based analysis for all the tweets of a specific hash tag. Any tweet containing the more dictionary based matching words is usually considered as the relevant tweet. If this hash tag is being discussed on social media it clearly follows a general trend. Any such tweet following a trend or being synchronous with other like tweets of a specific hostage is considered to be as non- hijacked tweet [26]. If the tweet is irrelevant then it has a good probability that it is a malicious because it is not following the talked trend of a specific hash tag. With around 20-30 hash tags training of the tool has been done. It gives a dictionary for the corresponding groups of specific hash tags. The output is based on high and low score tweets for a particular hash tag with high implying relevant and trending tweet with respect to specific hash tag and low implying a misleading one which of course uses a hash tag just for the sake of gaining attention [15].

Re-tweet Storm: Here, a tweet is instantaneously re-tweeted by several thousands of erstwhile bot based accounts; hence it is referred as re-tweet storm. It results in flagging or banning of original account, but the reposts & re-tweets are usually not getting deleted [24]. Parent or original account is usually known as the martyr bot, because it kind of sacrifices itself as it to spread the malicious bots [24].

In order to detect such Re-tweet Storms in a study, scrutiny of Twitter users allocating of official New York Storm Response Messages" uses inclusion based criteria [25]. They include every event tweets that-

(a) were actually pushed in the week surrounding some event by some selected accounts.

(b) contain few specific keywords [23, 25].

HTTP was the main C&C channel used by social bots in the early stages. To bypass firewall security HTTP based bots, attempt to hijack the communication channel. But these HTTP based botnets are still suffering from centralized issue. So it is very much possible that this centralized issue can be exploited in detection process [9]. Now the communication approach has been shifted to the advanced ones like on hash tags, encrypted text, friend requests, fraud clicks, videos, audio and so on due to various types of detection methods.

Now a days, images are frequently used in social networking websites; image based steganography methods are being used to encrypt the commands and other information inside an image, as a secure C & C based channel for communication on social networking sites [23]. Image steganography is a technique in which information is hidden or encrypted in images. The original image is known as cover image and new one is known as stego image.

Different techniques of image steganography are like detection of Straight Line Pixels (SLPs) used in Least and Significant Bit (LSB) method, Huffman coding technique, pixel value based differencing technique etc. For encryption purposes different encryption algorithms like DES, RSA etc are there for use. A lot of work has been done in this area to detect different social botnets. But there are certain open areas for social botnets, like image steganography, where focus is required. In this study apart from reviewing and analyzing various bot detection techniques, we are also proposing the use of machine learning based techniques to detect the stego images on several social media.

III. RELATED WORK AND LITERATURE SURVEY

As mentioned above, botnet, a network of computers which have been compromised as they are infected because of malicious kind code. They are controlled remotely under the supervision of common command with control (C&C) kind of channel by a Botmaster. Usually cyber criminals use social network as main platform for the malicious activities in the form of these social botnets and carry out the attacks like click fraud, DDoS, phishing and spamming. Apart from **hash tag hijacking** and **Re-tweet Strom** other types of botnet attacks are:

Spray and Pray: In this technique, the bots keep on posting links with a hope to get some clicks with each link. Programmatically text based posts generated by these bots is the main strength here so they are difficult to get detected by service radar of social network [24].

Click/Like Farming: For inflating follower's social bots are ideal, a marketing strategy designed to make a conversation or page look more popular. Various approaches have been proposed by researchers in order to analyze and detect them like in a study based on botnet detection with event-driven analysis" the event-driven based log analysis and the software system enables detection of infection due to botnet on the user's system [19, 23, 24].

Also in one of the study in relation to bot, it is used to determine main features and also, to improve the detection process of social bots C & C mechanism. The detection mechanisms used are server side and host side. From the server side point of view, it has been concluded that bot master textually encodes their commands, if social network has been used as C & C channel to determine, whether it is a suspicious message or not, differentiate between plain vs. encoded texts etc [23]. But an argument can be made here that these assumptions are not enough to cover majority of the scenarios. Firstly, it is not mandatory that text as means of encryption will be used by bots always; they may use steganography method [23]. Secondly, having number of textual encryption methods available these bots can create their own encryption ways, hence making it impossible for the server-side detection. However, in the host-side detection, three features of bots can be used: suspicious network traffic, self kind of concealment, and unreliable source in order to detect dubious bots [23]. As bots are being used by multiple processes, the assumption here is that a bot can do one process only in the host is not true always [14, 23].

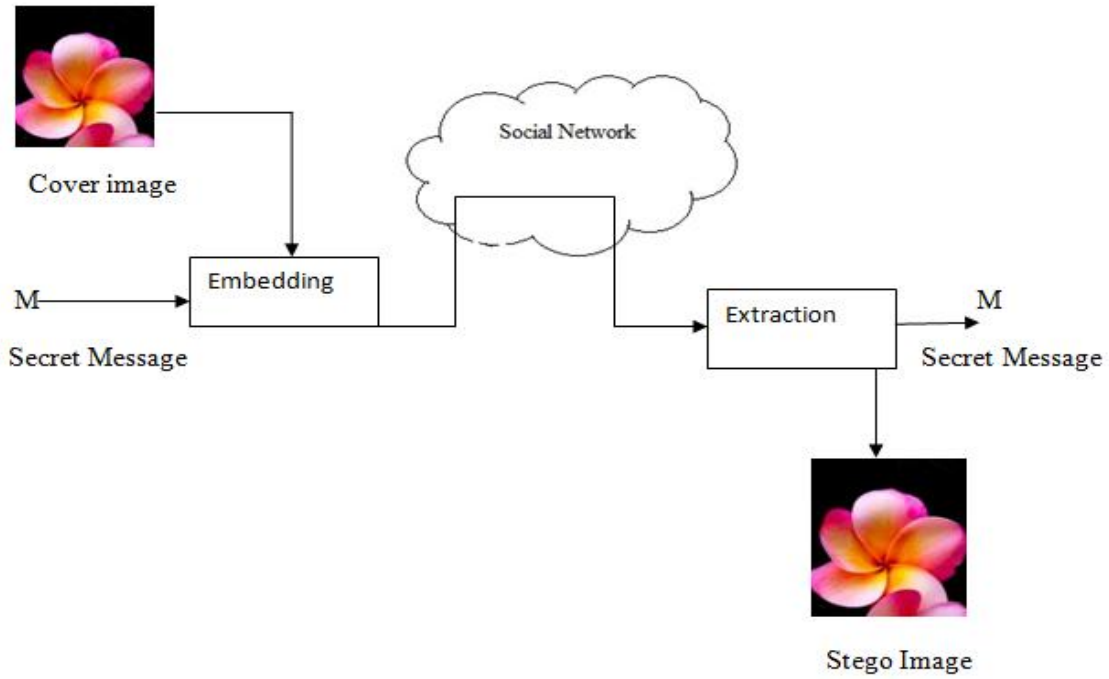

Fig. 1: General Scenario of Image Steganography

IV. RESULTS

As a result, botnets has emerged as budding threat, which is rising continuously in tandem with the rising dependence on online services of the users. With the advent of advance technologies based software's which are working in line with hardware resources, i.e. technology based on Internet-of-Things; botnets have now become attack within themselves, along with futuristic prospects. Thus, this study presents the effect of botnets on social media.

V. CONCLUSION

Social media botnets are a threat to the society and need to be tackled in a strategic manner. Thus effort has been made to identify different sets of techniques for handling the botnets and the different OSN sites having image datasets has been analyzed to find out whether those images are real images or stego images, by using different machine learning methods. With this approach images will be checked and stego images will be detected. By detecting the stego images on social networks we can stop the communication channels of social bots and we can detect the different botnets on OSN sites by recognizing their accounts that uploaded these images, thus shut down these bots. As stegano images are used for various malicious activities on OSNs, by detecting them we can stop large amount of such activities.

REFERENCES

1. Nazario J. Twitter based botnet command and control, <http://asert.arbornetworks.com/2009/08/twitter-based-botnet -command-channel>; 2009.
2. Anon Two million stolen facebook, twitter, yahoo, adp passwords found on pony botnet server,<http://www.zdnet.com/two-million-stolen-facebook-twitter-yahoo-adp-passwords-found-on-pony-botnet-server-7000023915/>; 2015.
3. Karasaridis, A., Rexroad, B., and Hoeflin, D.,." Wide-scale botnet detection and characterization" In Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets (Vol. 7), 2007.
4. Abu Rajab, M., Zarfoss, J., Monrose, F., and Terzis, A.. "A multifaceted approach to understanding the botnet phenomenon", In Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement (pp. 41-52). ACM, 2006.
5. Clayton Allen Davis, Onur Varol, Emilio Ferrara, Alessandro Flammini, and FilippoMenczer "Bot or not: A system to evaluate social bots" InProceedings of the 25th International Conference Companionon World Wide Web .International World Wide Web Conferences Steering Committee, 273–274, 2016.
6. Cheng Shao, Giovanni Luca Ciampaglia, Onur Varol, Alessandro Flammini, and Filippo Menczer, "The spread of fake news by social bots" ArXiv preprint arXiv:1707.07592, 2017.
7. Emilio Ferrara. "Manipulation and abuse on social media". ACM SIGWEB Newsletter Spring 2015.
8. V S Subrahmanian, Amos Azaria, Skylar Durst,Vadim Kagan, Aram Galstyan, Kristina Lerman,Linhong Zhu, EmilioFerrara, Alessandro Flammini and Filippo Menczer, "The DARPA Twitter bot challenge", Computer 49,6,38–46, 2016.
9. Zhao, David & Traore, Issa & Sayed, Bassam & Lu, Wei & Saad, Sherif & Ghorbani, Ali & Garant, Dan., "Botnet detection based on traffic behavior analysis and flow intervals". Computers & Security. 39. 2–16. 10.1016/j.cose.2013.04.007, 2013.
10. Yang Z, Wilson C, Wang X, Gao T, Zhao B Y, Dai Y. Uncovering social network sybils in the wild. ACMTrans. Knowl. Discov. Data 8(1):2, 2014.
11. Boshmaf, Yazan, et al. "Integro: Leveraging Victim Prediction for Robust Fake Account Detection in OSNs." NDSS. Vol. 15. 2015.
12. Chu, Zi, et al. "Who is tweeting on Twitter: human, bot, or cyborg?." Proceedings of the 26th Annual Ccomputer Security Applications Conference. ACM, 2010.
13. Tan E, Guo L, Chen S, Zhang X, Zhao Y. Spammer behaviour analysis and detection in user generated content on social networks, in: Distributed computing systems (ICDCS), IEEE 32nd International Conference on, IEEE, 20 12, pp. 305–314, 2012.
14. Kartaltepe, Erhan J., et al. "Social Network-based Botnet Command-and-Control: Emerging Threats and Countermeasures." International Conference on Applied Cryptography and Network Security. Springer, Berlin, Heidelberg, 2010.
15. Jain, Nikita, Pooja Agarwal, and Juhi Pruthi. "HashJacker-detection and analysis of hashtag hijacking on Twitter." International Journal of Computer Applications 114.19, 2015.
16. Rodriguez-Gomez, R. A., Macia-Fernandez, G., and Garcia-Teodoro, P., "Survey and Taxonomy of Botnet Research through Life-Cycle". ACM Computing Survey. 45, 4, August 2013.

17. K. Lee, B. D. Eoff, and J. Caverlee, “Seven months with the devils: A long-term study of content polluters on twitter.” in ICWSM, 2011.
18. D. C. Wu and W. H. Tsai, “A steganographic method for images by pixelvalue differencing,” Pattern Recognition Letters, Vol. 24, pp. 1613–1626, 2003.
19. T. S. Wang, C. S. Lin and H. T. Lin, “DGA Botnet Detection Utilizing Social Network Analysis”, International Symposium on Computer, Consumer and Control (IS3C), Xi’an, pp. 333-336, 2016.
20. M.A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "A multifaceted approach to understanding the botnet phenomenon," In Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement, pp. 41-52, 2006.
21. V. Yegneswaran, P. Barford, and V. Paxson, "Using honeynets for internet situational awareness," In Proceedings of the 4th Workshop on Hot Topics in Networks, College Park, MD, 2005.
22. Genes, Nicholas, Michael Chary, and Kevin Chason. "Analysis of Twitter users’ sharing of official New York storm response messages." Medicine 2.0 3.1 , 2014.
23. Yuede Ji, Yukun He, Xinyang Jiang, Jian Cao, Qiang Li “Combating the evasion mechanisms of social bots”,Computers & Security 58, 230–249, 2016.
24. Payal Chandak, Prof. H. P. Channe, “Design and Detection of Social Media Botnets using Event-Driven Analysis”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 5, May 2017.
25. Nicholas Genes, Michael Chary, Kevin Chason , ”Analysis of Twitter Users’ Sharing of Official New York Storm Response Messages”, Department of Emergency Medicine, Icahn School of Medicine at Mount Sinai, New York, NY, United States, 2014.
26. Nikita Jain, Pooja Agarwal, Juhi Pruthi, ”HashJacker- Detection and Analysis of Hashtag Hijacking on Twitter”, International Journal of Computer Applications (0975 – 8887), Volume 114 – No. 19, March 2015.

AUTHORS PROFILE

Dr. Amit Jain is working as an Associate Professor with Chandigarh University, Mohali. He is having 17+ years of teaching experience of educational institutions across India. He is member of several professional societies including IEEE, CSI, IAENG, STRA and IAOIP. He is currently working in the field of Data Sciences and is supervising 05 Ph.D. Research Scholars. His research interest includes Algorithms, Machine learning, Network Security and Artificial Neural Networks. He has currently 10 publications in renowned International Journals. Some of them are in Scopus Indexed Journals. Further, he has 20+ publications in several National and International Conferences. He has also published Book Chapter in internationally renowned publishing company named CRC Press. He is also serving as Reviewer for the various book titles from reputed publishers involving McGraw Hill, Pearson Education and Elsevier etc.

Dr Anand Kr Shukla, is having 15 years of related work experience, working as a associate professor and research coordinator in Chandigarh University, Mohali, India. Author of 5 books and more than 30 international publications. Dr Anand is also the member of Advisory Boards and Technical Program Committees of several IEEE and Elsevier's International Conferences. Have also the convener of an International Conference. Dr Anand is also the expert of Java & .Net having sound knowledge of Data Sciences, web engineering, and R language. Dr Anand have also the exposure of Software development and have delivered seminars, expert lectures in many Institutions and Universities.

Dr. Raju Kumar is working as an associate professor with Chandigarh University, Mohali, India. He has expertise in regular and online teaching, administration, and research activities. He received his doctorate in Computer Science from Gurukul Kangari Vishwavidyalaya, Haridwar, India. He did his master’s degree from Dr. Bhimrao Ambedkar University, Agra, India. He qualified UGC-NET in Computer Science and Applications. He is member of several professional societies including IAENG, IACSIT, CSTA, and IAOIP. His research interest includes distributed database, data science, machine learning, and ICT. He published several research papers in international and national journals and conferences. He has written and reviewed many Self Learning Material books for U.G and P.G Programmes.

.