2020 The 3rd World Symposium on Communication Engineering

AI-Powered Honeypots for Enhanced IoT Botnet Detection

Vasileios A. Memos
Dept. of Applied Informatics
University of Macedonia
Thessaloniki, Greece
e-mail: vmemos@uom.edu.gr

Kostas E. Psannis
Dept. of Applied Informatics
University of Macedonia
Thessaloniki, Greece
e-mail: kpsannis@uom.edu.gr

***Abstract*—Internet of Things (IoT) is a revolutionary expandable network which has brought many advantages, improving the Quality of Life (QoL) of individuals. However, IoT carries dangers, due to the fact that hackers have the ability to find security gaps in users' IoT devices, which are not still secure enough and hence, intrude into them for malicious activities. As a result, they can control many connected devices in an IoT network, turning IoT into Botnet of Things (BoT). In a botnet, hackers can launch several types of attacks, such as the well known attacks of Distributed Denial of Service (DDoS) and Man in the Middle (MitM), and/or spread various types of malicious software (malware) to the compromised devices of the IoT network. In this paper, we propose a novel hybrid Artificial Intelligence (AI)-powered honeynet for enhanced IoT botnet detection rate with the use of Cloud Computing (CC). This upcoming security mechanism makes use of Machine Learning (ML) techniques like the Logistic Regression (LR) in order to predict potential botnet existence. It can also be adopted by other conventional security architectures in order to intercept hackers the creation of large botnets for malicious actions.**

Keywords-botnet, DDoS, IoT, honeypots, malware spread, MitM

I. INTRODUCTION

Nowadays, the rapid growth of technology has increased the number of cybercrimes occurring worldwide and tends to become a pandemic. The great evolution of the Internet of Things (IoT), where all the physical objects tend to gain access to the internet, has caught the eye of hackers. A hacker can exploit the security gaps of IoT devices so as to gain unauthorized access into them. This is due to the fact that IoT devices have constrained resources and hence, only weak encryption algorithms can be applied, which make them vulnerable targets for attackers, or even a part of a botnet of compromised devices which carries out DDoS Attacks [1].

Therefore, hackers can use these IoT devices in order to make their own bot network (botnet) known as "zombie army", a network of many interconnected devices which can be used to launch Distributed Denial-of-Service (DDoS) attacks, Man-In-The-Middle (MitM) attacks, and spread various types of malicious software (malware). The more interconnected IoT devices, the greater potential for large botnets and huge number of attacks. According to research studies, botnets constitute the largest network attack worldwide [2].

In this paper we propose a novel security framework which can predict using Machine Learning (ML) the probability for an IoT device be a part of a botnet. The rest of the paper is organized as follows: Section II cites the latest related work; Section III analyzes the operation of botnets; Section IV presents the main countermeasures for detection and removal of botnets; Section V presents our proposed security framework and its evaluation; and finally, Section VI concludes the paper and gives potential future directions.

II. RELATED WORK

Last years, many research studies upon protection of IoT against botnets, have been conducted. A. Kumar and T. J. Lim [3] present an early botnet detection algorithm for IoT-Bots like Mirai family of malware in large-scale networks with analysis of sub-sampled packet traffic. In addition, T. Shah and S. Venkatesan [4] propose an effective technique to secure IoT devices against botnets and large-scale DDoS attacks. The authors implement a new method named as "login puzzle" which prevents from unauthorized login attempts came from malicious entities like malware scripts.

Several other studies demonstrate ML algorithms for optimized botnet detection rate. A. Prokofiev et al. [5] uses Logistic Regression (LR) model, a ML technique, which can improve the detection of IoT botnets. The same technique is used by R. Bapat et al. [6] for identifying malicious botnet traffic, in which experimental results show that their proposed method presents enhanced performance in terms of F-Measure, Accuracy ratio, and Area Under Curve (AUC) factors. F. Araujo et al. [7] implement a DEcEPtion DIGging (DeepDig) method which sets traps and decoys onto real computer systems and devices, and then, applies ML algorithm so as to provide a more comprehensive understanding of attackers' profile.

Other research studies focus on honeypot strategies to assess IoT cyberattack behavior [8]. Since honeypots have been designed to capture malware and zero-day attacks for a thorough analysis, there are many anti-detection methods developed by hackers in order to avoid falling into the trap of honeypot. S. Dowling et al. [9] use reinforcement learning so as to conceal honeypots functionality and improve their effectiveness against new malware variants. It is notable that honeypot strategy in combination with various ML techniques can be used to predict botnet existence [10]. In addition, Honeypot in combination with ML can be used to prevent hosts from zero-day DDoS Attacks [11]. Finally, Y. M. P. Pa et al. [1] propose an IoT honeypot (IoTPOT) and

978-1-7281-8564-4/20/$31.00 ©2020 IEEE

sandbox, which have the ability to capture and analyze Telnet-based DDoS attacks against different IoT devices.

III. Botnets Operation

A. Types of Botnets

There are several types of botnets, depending on what protocols and topologies they use. The basic types of botnets are the following [12]:

1) Centralized botnets

This structure has a single central Command and Control (C&C) server, where all the infected devices ("bots") are directly connected to this server. The attacker as botmaster uses the C&C server to send commands to all bots in the IoT network. Examples: IRC botnets and HTTP botnets.

2) Decentralized botnets

This structure has many C&C Servers which are the various infected devices used by the attacker as C&C servers for attacks. Example: Peer-to-Peer (P2P) botnets.

3) Hybrid botnets

Hybrid botnets use both centralized and decentralized model in order to take advantage of both of these structures. Hybrid botnets use encryption key so as to hide the botnet traffic within the normal traffic, making the attack more difficult to be detected in time.

B. Malicious Actions of Botnets

IoT as it is by own a large global network is regarded to be a perfect recipe for hackers to convert them to IoT botnets or Botnet of Things (BoT) [13]. Hence, a very large number of devices can be used by the malicious botmaster in order to spread malware or cause DDoS and MitM attacks [1].

A DDoS attack is a distributed denial of service attack where the attacker usually scans the IoT network and looks up for IoT devices with opened Telnet and SSH ports (host scanning) in order to gain access in the IoT device and inject a self-replicating script inside the vulnerable IoT device. This script is used to scan the whole network for other connected devices and inject the same script into them. When a satisfied number of infected devices (bots) are collected, the attacker can complete the DDoS attack, using a great mass of internet traffic [4]. The multiple connection requests to the target's server can set it out of order.

A Man in the Middle (MitM) Attack is a type of attack in which a third entity, namely the attacker, can intercept the network and eavesdrop all the exchanged messages between two parties like client and server, stealing sensitive information. Moreover, the attacker can inject false information and then intercept the exchanged data between the two entities [14].

If a compromised device is a part of a botnet, it may attract and spread various types of malware to other connected to an IoT network and even the whole network. As the botmaster can control the whole IoT network of the interconnected devices, he/she can inject with malicious code all the compromised devices whenever he/she wants. Therefore, the devices which are under a botnet may carry a lot of viruses, trojans, worms, spyware, ransomware, spamming, phishing, and other threats.

IV. Countermeasures Against Botnets

A. Defensive Methods

Generally, the most common defensive – detection methods for botnets are the following [12], [15-17]:

1) Signature-based technique

It uses signatures for recognizing specific known botnets which are stored in a database.

2) Anomaly-based technique

It has the ability to detect suspicious high network traffic with abnormal behavior which may caused by a botnet attack.

3) Host-based technique

It looks for bot like behavior in the host.

4) Network-based technique

It monitors the whole IoT network flow for bot activity at the early stage, while it can also detect directly unknown bots.

5) DNS-based technique

It merges signature-based and anomaly-based techniques, so as to analyze the collected data from DNS queries for botnet existence. It can also detect encrypted C&C servers.

6) Data mining-based techniques

These techniques use more powerful algorithms which can detect a botnet even in cases that the network traffic seems similar to normal traffic with low volume and low latency. Such algorithms are implemented using: machine learning, data classification, and clustering [18].

7) Honeynet-based detection

Honeynet is a network which is composed of more than one honeypot. A honeypot is either a real vulnerable machine or a virtual machine, which looks up for malicious servers and waits attacks. When it is infected, it records the attack and gives the network administrator a full clear image about the source and the methods of the attack. It is very difficult even for the most advanced attacker to avoid falling into the trap, because this trap is not a separate machine, device or software process, but within the real asset which is the attacker's target. Therefore, the defense mechanisms continually learn and are evolving at stopping even the stealthiest attacks [19].

B. Offensive Methods

The main offensive methods against botnets which focus on the elimination of botnets are the following [20]:

1) Bringing down C&C Server

As the C&C server is the command and control server from which the malicious botmaster can control and send commands to the whole network (e.g. an IoT network), the destruction of the root of the botnet can lead to the elimination of the whole botnet.

2) Sinkholing malicious traffic

If the first action cannot take effects, sinkholing or redirection of the malicious traffic to specific servers named as "sinkholes" may intercept the operation of the botnet.

3) Cleaning infected systems

Firewalls and up-to-date antivirus software can restrict and clean all the infected devices in an under-attack IoT

network respectively. However, many botnet malware can stay alive, as most users do not know that their IoT device is infected, and an automatic global cleanup is impossible.

V. Proposed Approach

A. Model Description

Our proposed approach is based on honeynet based detection method with the use of Artificial Intelligence (AI) for optimal botnet detection rate. It is remarkable that honeypots which are powered by AI offer many advantages. This is due to that AI makes honeypots rollout faster, less complicated and produces high-quality alerts [21].

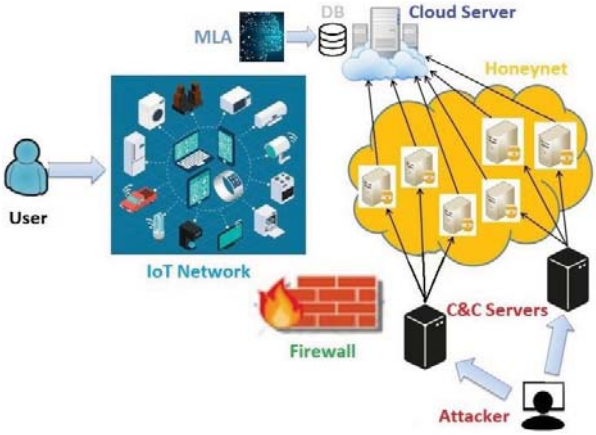

Figure 1. Botnet detection using AI-powered Honeypots.

Specifically, we propose a novel honeynet that is composed of many isolated honeypots, where each of them constitutes a vulnerable machine for waiting of botnet attacks. In other words, each honeypot operates as a decoy for attacks. Figure 1 illustrates our proposed scheme. Each honeypot is connected to a main robust Cloud Server where an advanced heuristic analysis of the attack is conducted. This analysis is based on data mining techniques, like classification and clustering, using Machine Learning Algorithm (MLA). The MLA is based on common events of botnet existence, and uses probabilistic methods and Deep Learning (DL) techniques from other recorded related infections stored in a Database (DB), in order to calculate the probability of botnet existence. After a thorough analysis, the Cloud Server returns the result to the administrator of the IoT network in order to take his/her countermeasures.

For calculations, we use the supervised Logistic Regression (LR) – MLA which might process input data to estimate the probability that a device is running as a bot, and therefore predict an infected host and network. For a regular botnet, the attacker runs a series of malicious commands in the C&C server. Based on the literature review, the most common commands are listed in Table I [8].

The command *iptables stop* turns off firewall and thus, the IoT device becomes vulnerable against both malicious users and software such as viruses, worms etc. Each *7* digit of the command *chmod 7777* means "read+write+execute" permissions. The last *7* extra digit gives elevated privileges on files and permits anyone to modify this file with administrative privileges. The *killall –9* command kills processes by name and hence, it may end up killing unrelated processes. The *rm –rf* command is one of the fastest ways to force delete a folder and its contents, and hence it may cause unrecoverable system damage. Wget is a software tool developed by the GNU Project and used in order to retrieve content and files from various web servers using HTTP, HTTPS, FTP and FTPS. Unfortunately, this tool is often installed by an attacker in order to download a script from a malicious website from a malicious source and then execute it into the host.

As it is shown in Table I, we have added an estimated weight according to the malicious action it makes. This value is calculated based on our estimated risk rate in a scale of 1-6, with 1 be a low risk and 6 a high risk action. The risk rates and weights are indicative, approximate, and may differ. Furthermore, they can be set and changed according to MLA and DL from related botnet threats.

B. Botnet Detection

As it is mentioned above, our proposed approach for detection botnets is based on honeypot infrastructure. After a possible attack, the collected information about this attack is sent to a Cloud Server where the possibility of botnet existence is analyzed. Thus, the executed commands and the corresponding actions that take place are examined.

TABLE I. Steps for Host Infection by Botnet Attack

ID	Parameter/ Command	Risk Rate (1-6)	Weight (0-1)	Action
#1	*iptables stop*	6	0.2857	Turn off Firewall
#2	*chmod 7777 (list of directories)*	5	0.2381	Change Permissions to directories
#3	*killall -9 (list of processes)*	4	0.1905	Kill processes
#4	*rm –rf (files and directories)*	3	0.1429	Delete Files and Directories
#5	*apt-get install wget*	2	0.0952	Install Wget Tool
#6	*wget http://malicious_source -O- | sh*	1	0.0476	Download and Execute Files

TABLE II. DSSParameterSetting

Detection Sensitivity Scale (DSS)	Overall Rate	Aggregate Weight Score
Very Low (VLS)	80%	0.80
Low (LS)	65%	0.65
Medium (MS)	50%	0.50
High (HS)	35%	0.35
Very High (VHS)	20%	0.20

For botnet existence, we use the metric of Detection Sensitivity Scale (DSS) classified into five scales: Very Low (VLS), Low (LS), Medium (MS), High (HS), and Very High (VHS), as it is shown in Table II. Thus, the network administrator will have the ability to set the sensitivity parameter in the Cloud Server.

Therefore, based on sensitivity parameter, the Cloud Server gives positive alarm for botnet existence. For example, the deactivation of the firewall of an IoT device (ID #1), according to Tables I & II, will be denoted as positive alarm only if the network administrator has set the DSS parameter on VHS. This is due to the fact that a possible firewall deactivation does not mean necessarily that the device is a bot.

In the case of observing an additional to the firewall deactivation, potential malicious action of changing permissions (ID #2), the LR-MLA gives an approximate 0.52 aggregate weight score, which means that even if the network administrator has set the sensitivity parameter on MS, the Cloud Server will give positive alarm for botnet existence. Figure 2 depicts the botnet existence probability using LR-MLA and DSS, if the potential malicious processes of Table I are applied step-by-step.

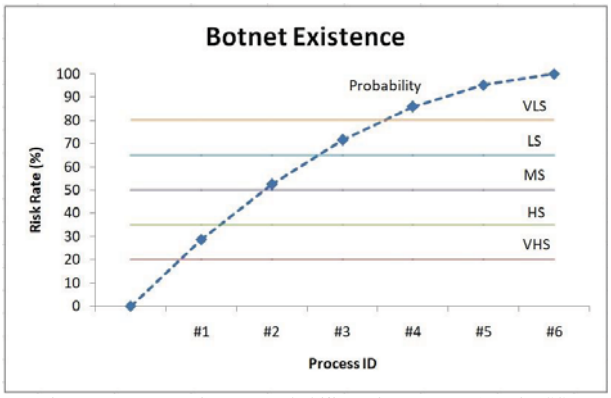

Figure 2. Botnet existence probability using LR-MLA and DSS.

C. *Effectiveness Evaluation*

At this point, we define the following meanings: True Positive (TP): shows that a malicious sample is correctly detected as malicious; True Negative (TN): shows that a non-malicious sample is correctly detected as non-malicious; False Positive (FP): shows that a non-malicious sample is falsely detected as malicious; and False Negative (FN): shows that a malicious sample is not detected and labeled as a non-malicious sample. Thus, we can estimate the effectiveness of our proposed model using the following performance metrics [5], [22-24]:

1) Accuracy (ACC): is the number of samples that a classifier correctly detects, divided by the number of all malware and non-malicious applications. It is defined as follows:

$$ACC = \frac{TP+TN}{TP+FP+TN+FN} \quad (1)$$

2) Precision or Positive Predictive Value (PPV): is the ratio of predicted malware that are correctly labeled a malware. It is defined as follows:

$$PPV = \frac{TP}{TP+FP} \quad (2)$$

3) Recall or Detection Rate or True Positive Rate (TPR): is the ratio of malware samples that are correctly predicted. It is defined as follows:

$$TPR = \frac{TP}{TP+FN} \quad (3)$$

4) Fall-out or False Positive Rate (FPR): is the ratio of non-malicious samples that are falsely detected as malware. It is defined as follows:

$$FPR = \frac{FP}{FP+TN} \quad (4)$$

5) F-Measure or Balanced F-score(F): is the harmonic mean of precision and recall. The more F-Measure closes to 1, the better it is. It is defined as follows:

$$F = 2 \cdot \frac{PPV \cdot TPR}{PPV+TPR} \quad (5)$$

Table III presents the effectiveness of the proposed model after the above calculations for each potential malicious process and each sensitivity scale. As it is clearly shown, for both MS and HS DSS, our proposed model could achieve the values of ACC 1.000 (100% rate), PPV 1.000 (100% rate), TRP 1.000 (100% rate), F-Measure 1.000 (100% rate), and FPR 0.000 (0% rate), if the security mechanism operates properly without bugs.

TABLE III. EFFECTIVENESS OF THE PROPOSED MODEL

ID	BOTNET	NON BOTNET	DETECTION SENSITIVITY				
			VLS	LS	MS	HS	VHS
#1	28.57%	71.43%	TN	TN	TN	TN	FP
#2	52.38%	47.62%	FN	FN	TP	TP	TP
#3	71.43%	28.57%	FN	TP	TP	TP	TP
#4	85.72%	14.28%	TP	TP	TP	TP	TP
#5	95.24%	4.76%	TP	TP	TP	TP	TP
#6	100.00%	0.00%	TP	TP	TP	TP	TP
ACC			0.667	0.833	1.000	1.000	0.833
PPV			1.000	1.000	1.000	1.000	0.833
TPR			0.600	0.800	1.000	1.000	1.000
FPR			0.000	0.000	0.000	0.000	1.000
F			0.750	0.889	1.000	1.000	0.909

VI. CONCLUSION

A novel security framework for improved detection of botnet existence is presented. Our proposed scheme makes use of emerging technologies like AI, ML, and CC in combination with honeynet-based detection method. This threat prediction model achieves efficiency in terms of Accuracy, Precision, Recall, Fall-out, and F-measure, and thus, it can be used for botnet detection.

Future work may include the implementation of such a security mechanism for evaluation of its robustness and effectiveness using analysis tools like the Botnet Detectors Comparer [25].

REFERENCES

[1] Y.M.P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "IoTPOT: A Novel Honeypot for Revealing Current IoT Threats", Journal of Information Processing, Vol. 24, Issue 3, pp. 522-533, May 2016.

[2] Y. Aleksieva, H. Valchanov, and V. Aleksieva, "An approach for host based botnet detection system", 16th Conference on Electrical Machines, Drives and Power Systems (ELMA), pp. 1-4, June 2019.

[3] A. Kumar and T.J. Lim, "Early Detection of Mirai-Like IoT Bots in Large-Scale Networks through Sub-sampled Packet Traffic Analysis", In: Arai K., Bhatia R. (eds) Advances in Information and Communication – FICC, Lecture Notes in Networks and Systems, Vol. 70, Springer, February 2019.

[4] Shah T. and Venkatesan S., "A Method to Secure IoT Devices Against Botnet Attacks", In: Issarny V., Palanisamy B., Zhang LJ. (eds) Internet of Things – ICIOT, Lecture Notes in Computer Science, Vol. 11519, Springer, June 2019.

[5] A. O. Prokofiev, Y. S. Smirnova, and V. A. Surov, "A method to detect Internet of Things botnets", IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 105-108, January 2018.

[6] R. Bapat, A. Mandya, X. Liu, B. Abraham, D. E. Brown, H. Kang, and M. Veeraraghavan, "Identifying malicious botnet traffic using logistic regression", Systems and Information Engineering Design Symposium (SIEDS), pp. 266-271, April 2018.

[7] F. Araujo, G. Ayoade, K. Al-Naami, Y. Gao, K.W. Hamlen, and L. Khan,"Improving Intrusion Detectors by Crook-sourcing", In Proc. 35th Computer Security Applications Conf. (ACSAC), December 2019.

[8] S. Dowling, M. Schukat, and H. Melvin, "A ZigBee honeypot to assess IoT cyberattack behaviour", 2017 28th Irish Signals and Systems Conference (ISSC), pp. 1-6, June 2017.

[9] Dowling S., Schukat M., and Barrett E., "Using Reinforcement Learning to Conceal Honeypot Functionality", In: Brefeld U. et al. (eds) Machine Learning and Knowledge Discovery in Databases, ECML PKDD 2018, Lecture Notes in Computer Science, Vol. 11053, Springer, January 2019.

[10] V. Mehta, P. Bahadur, M. Kapoor, P. Singh, and S. Rajpoot, "Threat prediction using honeypot and machine learning", International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), pp. 278-282, February 2015.

[11] R. Vishwakarma and A. K. Jain, "A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks", 3rd International Conference on Trends in Electronics and Informatics (ICOEI), pp. 1019-1024, April 2019.

[12] N. Kaur and M. Singh, "Botnet and botnet detection techniques in cyber realm", International Conference on Inventive Computation Technologies (ICICT), pp. 1-7, August 2016.

[13] E. Chickowski, "Hacker 2016 To-Do List: Botnet All The Things!", https://www.darkreading.com/iot/hacker-2016-to-do-list-botnet-all-the-things%21/d/d-id/1323759, May 2016, Last accessed: May 2020.

[14] E. Leloglu, "A Review of Security Concerns in Internet of Things", Journal of Computer and Communications, pp. 121–136, January 2017.

[15] S. Asha, T. Harsha, and B. Soniya, "Analysis on botnet detection techniques", International Conference on Research Advances in Integrated Navigation Systems (RAINS), pp. 1-4, May 2016.

[16] M. N. Sakib, and C. T. Huang, "Using anomaly detection based techniques to detect HTTP-based botnet C&C traffic", IEEE International Conference on Communications (ICC), pp. 1-6, May 2016.

[17] H. Ichise, Y. Jin, and K. Iida, "Detection Method of DNS basedBotnet Communication Using Obtained NS Record History", Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual, Vol. 3, July 2015.

[18] X. Dong, J. Hu, and Y. Cui, "Overview of Botnet Detection Based on Machine Learning", 3rd International Conference on Mechanical, Control and Computer Engineering (ICMCCE), pp. 476-479, September 2018.

[19] J. Leyden, "AI-powered honeypots: Machine learning may help improve intrusion detection", The Daily Swig: Cybersecurity news and views, https://portswigger.net/daily-swig/ai-powered-honeypots-machine-learning-may-help-improve-intrusion-detection, May 2020, Last accessed May 2020.

[20] F. Leder, T. Werner, and P. Martini, "Proactive Botnet Countermeasures – An Offensive Approach", The Virtual Battlefield: Perspectives on Cyber Warfare, Vol. 3, pp. 211-225, March 2009.

[21] M. Korolov, "AI-powered deception technology speeds deployment, improves results", https://www.csoonline.com/article/3537452/ai-powered-deception-technology-speeds-deployment-improves-results.html, April 2020, Last accessed May 2020.

[22] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset", Future Generation Computer Systems (FGCS), Vol. 100, pp. 779-796, November 2019.

[23] H. Nguyen, Q. Ngo and V. Le, "IoT Botnet Detection Approach Based on PSI graph and DGCNN classifier", IEEE International Conference on Information Communication and Signal Processing (ICICSP), pp. 118-122, September 2018.

[24] S. García, M. Grill, J. Stiborek, and A. Zunino, "An empirical comparison of botnet detection methods", Computers & Security, Vol. 45, pp. 100-123, September 2014.

[25] S. García, "Botnet Detectors Comparer", https://sourceforge.net/projects/botnetdetectorscomparer/, 2014, Last accessed June 2020.