RESEARCH ARTICLE OPEN ACCESS

An AI-Powered System for Identifying Network Threats

Mrunali A. Nikure

Assistant Professor, Dr S.G Gulhane Prerna College of Commerce, Science and Art
Nagpur, MS (India)

ABSTRACT

A network threat detection system called AI@NTDS is created by the project using the behavioral characteristics of attackers and cunning tactics. With the suggested AI@NTDS system, data analysis. The operating system or its operators can protect against network attacks using a simpler approach that uses feature extraction and evaluation to build a detection model. Telnet and SSH (Secure Shell) Linux system interaction data are sourced from the Cowrie Honeypot. and identified using MITRE ATT&CK Enterprise Tactics to guarantee the reliability of the dataset.

Based on the attacker's tactics and the user's risk of harm, the suggested AI@NTDS system has three tiers. The network threat level is detected using fifty-two features. The features include host-based features for all kinds of information in the network connection process, message-based features for various Linux operating instructions, and geography-based features that relate to the attacker's location. The K-NN algorithm, Random Forest, and Light GBM are AI-based algorithms that are used to confirm that the custom features have been identified.

Keyword:

Artificial Intelligence (AI), Cybersecurity, Threat, Detection, Machine Learning (ML).

I. INTRODUCTION

Artificial intelligence has emerged as a game-changing answer to these problems. Instead than depending on existing indicators, AI threat detection solutions use machine learning algorithms that are constantly evolving and improving, enabling them to identify previously unknown dangers through behavioral patterns. Large volumes of security data may be processed and analyzed by these systems at speeds and scales that are unattainable for human analysts, allowing them to spot minute irregularities that can indicate an impending intrusion.

In this study, AI-powered techniques are used to solve the command-based content problem and design a network threat detection system, AI@NTDS. Since an enormous amount of information is collected daily, the manual defense of the remote connection threats may cause an irreversible situation. The malicious command dataset for AI Model training is collected and organized by the Honeypot. Most importantly, the problem of detecting malicious commands is solved herein.

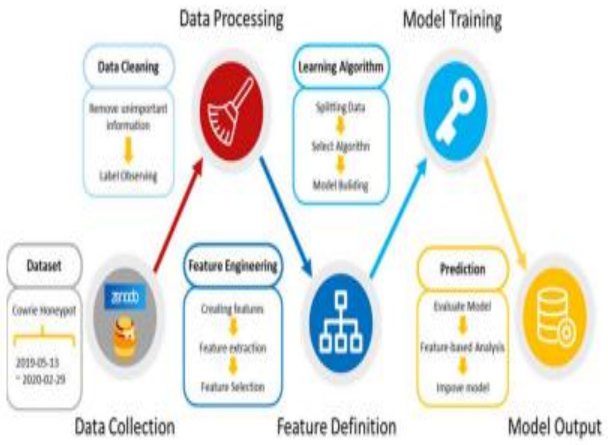
A. THE HONEYPOT THREAT IND ICATOR

Found that criminal activity on the Internet is becoming more sophisticated. Traditional information security technologies can barely cope with recent trends in such activity. In

this investigation, several Honeypots are combined to form a honeynet. The Honeynet ran for 222 days, and 12 million attack attempts were captured. The captured data are examined and evaluated herein. The experimental results can identify and quantify the dependences and distributions of the data. New threats are constantly emerging, so capturing the features of attacks and analyzing them effectively is essential. Several Honeypot sensors were deployed to monitor and study (the attackers' behavior. Honeypot type are in Cowrie, Dionaea, and Glastopf, in Linux hosts, Windows host, and web application environments. The above Honeypots attract various attacks from different environments.

B. NETWORK INTRUSION DETECTION SYSTEM DESIGN WITH AI

A machine learning-based intrusion detection system for software-defined networking (SDN). They used 41 features from NSL-KDD datasets for multi-class classification, and detected four kinds of attack DDoS, PROBE, R2L, and U2R.A heuristic distributed scheme (HIDE) to validate the falsification of traffic data. Their calculations were based on a homogeneous semi-Markov process that predicted the accuracy of mobility patterns. They used a cloudlet with a weight factor to determine whether a vehicle is malicious. To fill the gap between AI-based accomplishments and a comprehensive review of the cyber security threat landscape. They proposed and reviewed a machine-learning solution for threat detection and endpoint protection using deep reinforcement learning



C. DEEP LEARNING METHODS

Deep learning methods face stiff opposition in high-stakes security environments largely due to limitations in explain ability and murky interpretability issues. Researchers Wang and colleagues apparently conducted relevant studies.(2023) conducted a survey of security experts and discovered that not having model transparency was repeatedly mentioned as a top concern when adopting AI-based threat detection systems. A survey conducted in 2023 amongst numerous security experts unearthed a plethora of concerns regarding adoption of AI-based threat detection systems lacking transparency. Regulated sectors and government use cases face especially severe repercussions where legally mandated justification of decisions can be a necessity.

D. TYPES OF NETWORK SECURITY THREATS

The types of network security threats mainly include malware, denial-of-service attacks (DDoS), phishing, and packet sniffing.

(1) Malicious software: Malicious software includes files or programs that damage and

destroy the computer. Such as ransom software, zombie software, spyware, trojan horses, viruses or worms, etc., which will provide hackers with unauthorized access and cause damage to the computer.

(2) Denial of service attack (DDoS): DDoS is a malicious act that floods the target server or surrounding infrastructure with large scale network traffic, thereby disrupting the normal traffic of the target server or network.

(3) Phishing: Phishing induces users to provide personally identifiable information or sensitive information, such as online fraud, which is through emails or text messages disguised as formal and legal, requiring users to provide bank cards, passwords and other private information.

(4) Data packet sniffing: Data packet sniffing is a kind of eaves dropping attack that intercepts normal network communication data, then performs data tampering and sniffing, but the two parties to the communication do not know about it.

E. ANALYSIS OF AI@NTDS SYSTEM

The test dataset comprises 23% of the data in all experiment datasets. The training set comprises data from 2019, and the test set consists of data from 2020. The AI@NTDS classifier predicts the classification of each threat in the test dataset, yielding the results in Table 11. From the confusion matrix, the total misclassification ratio of the classifier for threat level 1 is 0.17%; that for threat level 2 is 0.37%, and that for threat level 3 is 0.86%. The F1-score reaches 99.80%, indicating that the AI@NTDS effectively detected samples of various threats. The AUC (Area Under the Curve) reaches 98.53%; the precision rate can reach es 99.75%, and the recall rate reaches 99.85%. Therefore, the detection model that is trained using the Light GBM algorithm can detect malicious sample changes in various periods of attack and has excellent efficiency and performance.

Comparison with related works.

	Proposed AI@NTDS System	Classification of SSH Attacks Using Machine Learning Algorithms (2016)	Attack detection and forensics using honeypot in iot environment (2019)	Detection of Malicious Remote Shell Sessions (2019)	Identification and classification of cyber threats through ssh honeypot systems (2020)	A novel Machine Learning-based approach for the detection of SSH botnet infection (2021)
Goal	Classification by level	Classification by malicious and benign	Classification by attack type	Classification by malicious and benign	Classification by level	Classification by infected and uninfected
Message	✓			✓	✓	✓
Host	✓		✓		✓	
Network		✓				✓
Geography	✓		✓		✓	

CONCLUSION

This study proposed an AI@NTDS detection system that incorporates the Light GBM machine learning algorithm for identifying and classifying threats. Attackers' intentions are analyzed using collected data, and the degree of harm that is caused by malicious instructions is determined. Three types of attack are identified by threat levels of attack are identified using Enterprise Tactics of MITRE ATT&CK. A total of 52 features of three types - message-based, host-based, and geography-based features - are ultimately identified. The results of an analysis demonstrate that our model performed best when all features were used. Message-based features and host-based features accuracy for the model are largest.

REFERENCE

[1]. Fraunholz, M. Zimmermann, A. Hafner, and H. D. Schotten, ‘‘Data mining in long-term honeypot data,’’ in *Proc. IEEE Int. Conf. Data Mining Workshops (ICDMW)*, Nov. 2017, pp. 649–656

[2]. Kyriakou and N. Sklavos, ‘‘Container-based honeypot deployment for the analysis of malicious activity,’’ in *Proc. Global Inf. Infrastruct. Netw. Symp. (GIIS)*, Oct. 2018, pp. 1–4

[3]. Sentinel One– Autonomous threat prevention platform.

[4]. S. Iranmanesh, F. S. Abkenar, A. Jamalipour, and R. Raad, ‘‘A heuristic distributed scheme to detect falsification of mobility patterns in internet of

[5]. vehicles,’’ *IEEE Internet Things J.*, vol. 9, no. 1, pp. 719–727, Jan. 2022.

[6]. M. Sewak, S. K. Sahay, and H. Rathore, ‘‘Deep reinforcement learning for cybersecurity threat detection and protection: A review,’’ in *Proc. Int. Conf. Secure Knowl. Manage. Artif. Intell. Era*, vol. 1549, 2021, pp. 51–72.

[7]. R. K. Shrivastava, B. Bashir, and C. Hota, ‘‘Attack detection and forensics using honeypot in IoT environment,’’ in *Proc. Int. Conf. Distrib. Comput. Internet Technol.*, Jan. 2019, pp. 402–409.

[8]. P. Dumont, R. Meier, D. Gugelmann, and V. Lenders, ‘‘Detection of malicious remote shell sessions,’’ in *Proc. 11th Int. Conf. Cyber Conflict*, May 2019, pp. 1–20.

[9]. S. Udhani, A. Withers, and M. Bashir, ‘‘Human vs bots: Detecting human attacks in a honeypot environment,’’ in *Proc. 7th Int. Symp. Digit. Forensics Secur. (ISDFS)*, Jun. 2019, pp. 1–6.

[10]. T.-H. Lee, L.-H. Chang, and C.-W. Syu, ‘‘Deep learning enabled intrusion detection and prevention system over SDN networks,’’ in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6.

[11]. J. M. J. Valero, M. G. Pérez, A. H. Celdrán, and G. M. Pérez, ‘‘Identification and classification of cyber threats through SSH honeypot systems,’’ in *Handbook of Research on Intrusion Detection Systems*. Hershey, PA, USA: