IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

Cyber Guardian : Intelligent Threat Surveillance

Aditi. H. R.[1], Anusha Bhaskar D[2], Priyanka. H. V.[3]
Undergraduate Students, Department of Information Science and Engineering[1,2]
Assistant Professor, Department of Information Science and Engineering[2]
Global Academy of Technology, Bangalore, India

Abstract: *Advanced persistent threats (APTs) are cyberattacking that use covert strategies to target specific groups. As a result of the rapid growth of computing technology and the widespread connectivity of devices, there has been a boom in data transfer across networks. Because APTs' attack tactics are always changing, it can be difficult to detect them. This has led cybersecurity experts to develop creative solutions. We found gaps in the research on APT detection by doing a systematic literature review (SLR) covering the years 2012 to 2022 and finding 75 studies related to computer, mobile, and Internet of Things technologies. The most sophisticated cyberattack, known as an advanced persistent threat, involves malevolent individuals breaking into a network without authorization and staying hidden for an extended period. Advancement persistent threat attacks and organizational threats are becoming more frequent. Machine learning is one technique used to detect attacks by sophisticated persistent threats. The need for improved detection methods is highlighted by our findings, and we offer suggestions to guide the creation of early APT detection models and progress in cybersecurity. We propose a conceptual model known as Cyber Guardian that uses Random Forest classifier and attention techniques to create a self-translation machine through an encoder-decoder framework. These advanced attention algorithms are intended to improve the machine's capacity to examine and decipher intricate patterns found in HTTP requests, enhancing APT detection capabilities, and providing cybersecurity experts with cutting-edge instruments to proactively detect and neutralize new threats in real-time. This all-encompassing strategy is a major advancement in the ongoing fight against Advanced Persistent Threats (APTs) and emphasizes how crucial it is for the cybersecurity community to continuously innovate and collaborate in order to remain ahead of changing cyberthreats.*

Keywords: web application attack, advanced persistent threat, APT malware, Network traffic, Cyber Security, Cyberthreats.

I. INTRODUCTION

Data are specific facts, figures, or information that are mainly numerical and essential to contemporary computing and mobile applications. Worldwide internet users increased by 7.6% in 2021 to account for 60% of the worldwide population, producing a massive daily data volume of roughly 1.145 trillion gigabytes. In networking, data are divided into packets, which are made up of control data (headers and trailers) that provide routing information and user data (payloads) that contain meaningful content. IP payloads are typically 64 KB in size, while Ethernet packets are typically 1.5 KB. Although packets moving over networks are referred to as network traffic, it's important to remember that malevolent actors might take advantage of weaknesses by creating malicious traffic in order to overwhelm or compromise networks.

The necessity of a wireless network environment that is mobile has led to the essentiality of smartphones. The location of the user, call records, and financial and personal data are among the data kept in a smartphone [4]. Smartphones have limited resources [5], are small, and operate heterogeneous services [4] in addition to being mobile. As a result of the absence of security safeguards, user data kept on cell phones is vulnerable to leakage and disruption. Advanced persistent threats (APTs) and other cyberthreats have made cell phones a popular target as a result [5].

Techniques such as sandboxing, aberrant network activity analysis, and full-flow detection that are currently in use to identify Advanced Persistent Threat (APT) attacks have accuracy issues and typically focus on certain stages of the attack cycle. A comprehensive security detection system [11] that covers every stage of an APT assault and uses a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

tiered monitoring strategy for various data sources and network protocols is desperately needed to address these issues. Casting a wide net, this comprehensive method aims to improve detection capabilities by making it more difficult for attackers to completely avoid detection. Through the use of this strategy, entities can enhance their protection against complex and enduring cyber-attacks.

Antiquated cybersecurity measures like firewalls and intrusion detection systems (IDSs) are insufficient to stop Advanced Persistent Threat (APT) attacks because they rely on social engineering techniques to trick trustful people into giving hackers access. Because APT attacks are dynamic and sophisticated in nature, unlike conventional cyber threats, typical security measures are unable to identify or prevent them. These attacks are always changing, using cutting-edge methods to get beyond established defenses.

It can be difficult to find APT malware in a network setting. First, timely detection is challenging due to the growing amount of network data and the proliferation of connected devices. The massive volume of traffic makes it resource-intensive to monitor events throughout the whole network and makes it difficult to differentiate between APT assaults and normal traffic. Furthermore, because hacking tools and techniques are always evolving, APT malware patterns also do, which means that detection engines must be able to quickly adjust to these changes. Secondly, most packets—including those that might contain malicious activity—are encrypted when utilizing HTTPS to establish secure internet connections. Tools like Tor, which encrypt and tunnel traffic over distributed server networks, further obfuscate the identity and actions of attackers. Consequently, harmful network traffic [13] that is encrypted may be present on even protected internet communication channels. Thirdly, because multistep APT attacks are so complicated, intrusion detection systems (IDSs) could have trouble identifying them even when they analyse attack behaviour. Comprehensive analysis is necessary for the detection of APT attacks, which occur throughout various stages of the attack life cycle. This complicates comprehensive APT detection, though, as research frequently focuses on discrete stages. It's still difficult to differentiate between benign abnormalities and APT attacks, which causes false positives and impedes the discovery of real threats. To tackle these issues, adaptive detection methods that can distinguish between changing APT strategies in encrypted traffic and multistep attack sequences are necessary.

II. APT DETECTION TECHNIQUES

The ability to evade traditional security measures like firewalls and antivirus software is possessed by Advanced Persistent Threats (APTs). A multilayered defense plan and the correlation of data from different security technologies are essential in the fight against them. Pattern-matching-based detection techniques [15], which identify recognized threats, and anomaly-based detection techniques, which identify anomalous activity, are the two main types of detection methods used for APTs. Integrating these strategies improves an organization's capacity to identify and neutralize APT threats. There are few papers which describe about APT detection techniques.

2.1 A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model [1]

In this study they divided the dataset into training, validation, and test sets in order to apply machine learning algorithms. While validation evaluates the adequacy of the model and modifies its hyperparameters, training is used to modify parameters and train the model. Test sets offer an objective assessment of the finished model. A range of metrics, including F1-score, precision, recall, and accuracy, are used to evaluate the method's performance.

Gathering network traffic data for analysis is the initial phase in the process, known as data collection. This is necessary to create efficient malware detection algorithms, especially for Advanced Persistent Threats (APTs). The objective is to gather datasets that are harmful as well as benign, with the empirical nature of the data typically determining how effective the results are.

The cybersecurity detection engine extracts desirable features (such IP addresses) from the gathered data in the second step, which is referred to as feature extraction. Important properties, which might be either static or dynamic, are categorized using this technique. The most crucial elements are then chosen and prioritized using feature reduction techniques.

Detection, the third phase, uses appropriate machine learning (ML) models to distinguish malicious packets from benign ones. APT detection using machine learning techniques includes anomaly detection, pattern recognition,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

classification, and training data clustering. In order to protect network security, the cyber defense system either notifies network managers when dangerous packets are discovered or blocks them.

Advantages:

The method combines a number of performance evaluation indicators, including F1-score, precision, recall, and accuracy, to enable a thorough evaluation of the method's efficacy and ongoing improvement.

Disadvantage:

Traditional intrusion detection systems have difficulty identifying novel APT patterns or malevolent traffic exhibiting unfamiliar characteristics, such as zero-day attacks, while simultaneously reducing false positives. For better detection, machine learning is advised, especially ensemble learning. When many machine learning techniques are combined, ensemble learning takes advantage of their advantages to provide results that are more accurate than when only one method is used.

2.2 APT Beaconing Detection: A Systematic Review [2]

In our review, we found that the most commonly used APT detection approaches include network flow analysis, signature-based detection, graph-based methods, game-based methods, and event correlation analysis. While other methods like blacklisting, whitelisting, and memory analysis are less common, they can still be integrated with the primary detection techniques to enhance the overall effectiveness of APT detection systems.

A predetermined collection of recognized signs of Advanced Persistent Threat (APT) attacks is the foundation of signature-based detection. These signs include a range of features, including file hashes, known byte sequences, malicious sites, email subject lines, and network behaviours. By comparing observed patterns with this list of signatures, the approach works. Its efficacy is limited to known threats, though, therefore it is insufficient against unknown or new APT attacks.

Unlike signature-based techniques, network flow analysis-based detection looks for unusual activities in network traffic. In this procedure, normalized and standardized network behavior is used to train detection systems, which are then used to monitor ongoing network activity. Alarms are set off by departures from the standard, indicating possible security incidents. This strategy is useful for identifying dangers that were previously undiscovered and that signature-based techniques might miss.

Another method for finding APT abnormalities in large datasets is graph-based anomaly detection. Using this strategy, features of an APT attack are revealed through data analysis in the form of a graph. It has specific mechanisms to deal with abnormal data, which can be hard to find using traditional data mining methods. Typically, supervised, unsupervised, or semi-supervised techniques are used by graph-based systems to provide efficient anomaly detection in a variety of scenarios.

Game-based techniques examine conflicts of interest between APT attackers and protecting systems by utilizing game theory concepts. These techniques investigate several approaches intended to reduce the dangers related to APT assaults. As an example, a generalized family of matrix games is studied as a possible risk reduction method. Furthermore, in situations when players could not fully understand each other's strategies or reward functions, Bayesian game strategies are used. In dynamic contexts, these techniques help defenders predict and counteract APT threats.

Techniques for detecting beaconing and APTs during APTs include:

Behavior based/network-based detection: This approach is predicated on host behavior or aberrant network traffic, which includes anomalous system behaviors, high traffic volumes, odd port activity, and excessive network latency. This method's objective is to spot any divergence from innocuous activity or behavior that resembles C&C behavior.

Advantages:

The method identifies APT and beaconing attack traits, enabling effective detection. It offers seamless integration into existing systems, enhancing overall cybersecurity.

Disadvantages:

Expensive or intricate execution.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

2.3 An Approach for Detection of Advanced Persistent Threat Attacks [3]

The paper's methodology suggests a top-down way for identifying Advanced Persistent Threat (APT) attacks. It entails building the methodology, which gathers and examines configuration files and system logs. Data analysis is used to identify APT approaches, which are then matched to particular strategies kept in an APT repository. Each attack step's techniques are identified by the APT technique identifiers and subsequently matched to established strategies by the APT matcher. This mapping is used to generate APT instances, which are then ranked by an APT ranker according to their completeness.

Advantages:

The technique offers a thorough framework for detecting APTs, encompassing both generic and particular APT techniques. To help with effective APT attack identification and response, it has automated analysis phases.

Disadvantages:

The accuracy and completeness of the APT repository, which comprises strategies that are well-known, will have a major impact on how well the suggested method for APT detection performs. Any errors or holes in this repository could make it more difficult for the system to recognize novel or evolving APT techniques, which could jeopardize the system's overall effectiveness. Furthermore, the intricacy of the suggested approach poses difficulties for both execution and upkeep. Data parsers, identifiers, matchers, and rankers are just a few of the many components that could make the integration and administration process difficult and time-consuming. Due to its complexity, the detection system may need to be optimized and require a significant time and skill commitment to assure proper operation.

2.4 Advanced Persistent Threat Identification with Boosting and Explainable AI [4]

Dataset Description: 315,607 rows and 84 attributes make up the SCVIC-APT-2021 dataset, which is derived from [20]. This dataset is used to detect Advanced Persistent Threats (APTs) in network traffic. Six class labels, each corresponding to a different APT activity, are included in the dataset.

Pre-processing of Data: Pre-processing procedures for the original dataset included handling null values, handling duplicates, label encoding for categorical data, column removal, and min-max normalization for data scaling. Because distance-based approaches were not used in the studies, normalization was selected over standardization.

Accelerating Formulas: Gradient Boosting and AdaBoost are two examples of boosting-based machine learning classification approaches used in the study. By using gradients to reduce prediction errors or iteratively modifying weights, these techniques seek to improve the performance of weak learners. Furthermore, an analysis was done comparing LightGBM, XGBoost, and CatBoost.

Advantages:

The dataset SCVIC-APT-2021 offers a comprehensive collection of network traffic data tagged with APT activity labels, making it a solid basis for assessing detection methods. The dataset is prepared for machine learning research, guaranteeing consistent scaling and dependability, by means of rigorous pre-processing procedures that handle null values, duplicates, and categorical data, as well as normalize features. Furthermore, by including a variety of data patterns and subtleties into the model training process, flexible boosting techniques like Gradient Boosting and AdaBoost might potentially improve detection performance.

Disadvantages:

Large dataset management can be difficult during pre-processing steps like feature engineering and normalization, which increases computational overhead and complexity. In order to effectively maximize detection performance, choosing the best boosting techniques also necessitates carefully evaluating task requirements and dataset features. Nevertheless, the interpretability of ensemble models produced by boosting techniques might make it challenging to see the underlying patterns and choices, which would limit our ability to comprehend classifier behavior and interpret the models.

2.5 A novel approach for detecting advanced persistent threats [5]

Data Source and Collection Methods: During the course of four months, packet capture was employed to gather information on attacks by Advanced Persistent Threats (APTs). To create unique network traffic, a variety of attack scenarios were simulated, including lateral movement, data exfiltration, compromise, and reconnaissance. Cyber Threat

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

Intelligence (CTI) sources and Security Information and Event Management (SIEM) systems provided about 42,000 tagged traffic logs.

Pre-processing of Data: Using complete case analysis to handle missing values, Min-Max scaling for normalization, and feature extraction to characterize the dataset according to attack scenarios, IP addresses, ports, and protocols were the pre-processing processes involved.

Extraction of Features: Based on attack scenario timing, IP addresses, ports, and protocols, features were taken out of the dataset. Key properties were identified by generating a heatmap of features from a CSV file containing labeled data. To identify important attributes, a feature importance analysis was done.

Feature Selection: In order to minimize data dimensionality, 14 features with zero instances were deleted and four features were removed to prevent bias. The dataset was optimized for classification using six feature selection techniques: ANOVA, chi-square, FFS, RFS, XGB, and Lasso.

Advantages:

A comprehensive analysis of network traffic behavior is made possible by the large dataset, which offers a wide variety of APT assault scenarios. Effective pre-processing methods guarantee data quality and consistency, which improves the dependability of ensuing studies. By determining which features are most pertinent for detection, feature selection optimization techniques also maximize classification performance.

Disadvantages:

Significant computer resources may be needed to handle huge datasets and execute numerous feature selection algorithms.

2.6 Locate-Then-Detect: Real-time Web Attack Detection via Attention-based Deep Neural Networks [6]

The module of the LTD system called Payload Locating Network (PLN) is in charge of locating questionable areas inside bulk requests or messages. The goal of the PLN's analysis of incoming web traffic is to identify regions that might harbour harmful payloads or signs of online attacks. Initially, the Payload Classification Network (PCN) narrows down the field of analysis through the use of the PLN as a filter.

The LTD system's primary component, the Payload Classification Network (PCN), is in charge of precisely categorizing and identifying attacks coming from the dubious areas that the PLN has detected. The PCN assesses the contents of the detected payloads using cutting-edge machine learning techniques to identify whether they are malicious or valid traffic. Through efficient separation of benign from malicious payloads, the PCN significantly improves the system's overall security posture.

Web Attack Annotation: In this component, web attacks that are utilized for training and assessment are annotated inside the dataset or traffic logs. The LTD system uses it as a reference to learn and identify patterns linked to different kinds of online attacks. For the PLN and PCN modules to be trained efficiently and be able to recognize and categorize attacks with a high degree of precision, accurate annotation is necessary.

Locate-Then-Detect (LTD) Mechanism: The PLN and PCN modules are part of the Locate-Then-Detect system, which works in concert to effectively detect web threats. After the PLN has identified suspicious regions in the online traffic, the detected payloads are next examined and categorized by the PCN in order to detect possible attacks. The LTD system takes a step-by-step approach, first detecting areas of concern and then using classification methods to ascertain the type of payloads present in those areas. This methodology improves the efficacious detection and mitigation of web-based threats by the system.

Advantages:

Scalability and flexibility are made possible by the LTD system's modular design. To make maintenance, upgrades, and integration with current security infrastructure easier, each module—PLN and PCN—focuses on particular activities.

Disadvantages:

It can only deal with SQL Injection and XSS attacks currently.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

2.7 Web-APT-Detect: A Framework For Web-Based Advanced Persistent Threat Detection Using Self Translation Machine With Attention [7]

The training phase involves the following steps for processing one HTTP request:

Token parse: HTTP requests are split into token sequences based on punctuation, generalizing unimportant information to reduce vocabulary size.

Building vocabulary: Convert all HTTP requests in the training dataset into token sequences. Select tokens exceeding a frequency threshold to build the vocabulary.

Training model: Input the token sequence into the self-translation machine, obtain the translated result, calculate the difference between input and output sequences (loss function), and use a backpropagation algorithm to adjust model parameters.

The key steps of anomaly detection are as follows:

Token parse: HTTP requests are segmented into token sequences based on punctuation.

Vocabulary: Utilizing the vocabulary generated in the training phase, transform the token sequence into the corresponding vocabulary ID sequence.

BLEU metric: Employ the BLEU score [9] to measure the difference between the input token sequence and the translated token sequence. The BLEU score ranges from 0 to 1, with higher scores indicating better translation quality. A threshold, denoted as, is defined. If the BLEU score is less than we categorize the translation quality as poor, marking the input HTTP request as anomalous.

Attention Mechanism:

Following the token parsing and vocabulary steps, the original HTTP request is converted into a token sequence, denoted as x, for further processing by our model.

Advantages:

Experiments on the CSIC2010 dataset show that the method obtains a remarkable F1-Score of 0.9844. This performance outperforms existing algorithms and competes with cutting-edge supervised learning models, demonstrating the algorithm's high accuracy web attack detection capabilities.

Disadvantages:

The use of sophisticated methods like the attention mechanism and self-translation machine could make the design and operation of the algorithm more complex. It may be difficult for organizations with little funding or experience in machine learning to implement and use the algorithm efficiently.

2.8 A Comprehensive Detection Method for the Lateral Movement Stage of APT Attacks [8]

The authors collected 10,000+ malicious files from VirusTotal and Aliyun TIANCHI datasets, spanning various malware types. They simulated sandbox behaviour to gather API command sequences, categorizing them into 8 tags based on malware type. For feature engineering, they pre-processed data, extracted features from API sequences, and used TF-IDF to convert them into numeric features, aiding in distinguishing between malware types.

The experimental setup utilized Tensorflow and Scikit-Learn libraries to implement the neural network model, employing a GTX2080 Ti GPU. Data was split into a 7:3 ratio for training and testing, with further subdivision into training and validation sets using 5-fold cross-validation. An early stop mechanism was implemented during training to prevent overfitting. Evaluation metrics included cross-entropy loss function and accuracy rate. Following 5-fold cross-validation, the model achieved a training set loss of 0.43 with an accuracy rate of 85% and a test set loss of 0.28 with an accuracy rate of 98%. Comparative analysis against TextCNN, FastText, and TextCNN + LSTM models demonstrated superior performance of the proposed model, attributed to its attention mechanism. Future work could focus on optimizing parameters and network structure to improve efficiency and accuracy.

Advantages:

Through extensive experimentation and comparison with benchmark models like TextCNN and FastText, the proposed model demonstrates superior performance in terms of accuracy and loss reduction, indicating its effectiveness in identifying different types of malwares.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

Disadvantages:
The proposed neural network model, while effective, requires significant computational resources due to its large number of parameters and complex architecture. This could limit its practical applicability, especially in resource-constrained environments.

2.9 A novel approach for APT attack detection based on combined deep learning model [9]
Three primary processes are involved in the suggested APT assault detection methodology. The CICFlowMeter tool is used in Step 1 to analyse network traffic into flow networks and extract 76 flow behaviour parameters, including FlowID, Source IP, Destination IP, and Packet Length. After that, these flow networks are paired together into source and destination IP pairs and arranged chronologically. In Step 2, CNN-MLP and CNNLSTM mixed deep learning models are used to extract IP features based on the flow networks. Finding characteristics common to both regular IPs and APT IPs is the goal of this stage. The specific steps involved in obtaining IP features are explained. In order to identify APT attacks, IPs are categorized in Step 3 using the attributes that were extracted in Step 2.
Advantages:
By combining MLP, CNN, and LSTM deep learning networks into a cohesive affiliate network, the proposed model achieves superior results compared to individual deep learning networks. This demonstrates the effectiveness of leveraging combined deep learning architectures for feature extraction and IP classification.
Disadvantages:
The paper acknowledges the need for further research to optimize the selection and optimization of features in combined deep learning models and machine learning algorithms for IP classification. This suggests that while the proposed method shows promise, there are still areas for improvement and refinement in future studies.

2.10 Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis [10]
The training dataset construction involved gathering around one thousand domains utilized as command and control (C&C) servers for crafted malware, alongside an equal number of benign domains. The malicious domains were sourced from platforms like malwaredomains.com and VRTrulesets, as well as extracted from malware samples detected by our institution's Virus Email Detector System. We specifically focused on C&C server domains for crafted malware, excluding domains generated by malicious flux or Domain Generation Algorithms (DGAs). Over a four-week period, we meticulously observed the time-based behavior of these malware C&C domains and manually labeled approximately 500 malicious domains and over 200 infected machines within our network. Each domain and IP address designated as malicious underwent thorough verification by network administrators. Furthermore, we incorporated one thousand benign domains obtained from the Alexa top 1000.
The Malicious DNS Detector classifier utilizes the J48 decision tree algorithm, which is based on the C4.5 algorithm. This decision tree classifier has demonstrated efficiency in distinguishing between benign and malicious domains, as shown in the EXPOSURE study. During the training period, the J48 decision tree classifier is constructed, with each node examining the condition of specific attributes. The branches of the tree represent the outcomes of this examination.
The reputation engine assesses whether network hosts display behaviour indicative of malware infection based on their IP addresses. It computes a reputation score ranging from 0 to 1, where 0 represents low reputation (likely infected) and 1 represents high reputation (clean). The engine utilizes three modules to generate feature vectors: malicious DNS detection, signature-based detection, and anomaly-based detection. These vectors are concatenated and fed into a trained reputation function, which outputs the reputation score. The function is trained using a dataset of feature vectors labeled with infection status.
Advantages:
IDnS reduces the volume of network traffic that needs to be recorded and analysed, particularly beneficial for large and high-speed networks. This optimization enhances the sustainability of the system by alleviating the burden of processing vast amounts of inbound and outbound traffic data.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

Disadvantages:

IDnS faces challenges in detecting malware infections that do not depend on domains, like trojans using direct IP addresses for command and control. This limitation hampers its effectiveness in identifying certain types of malware threats. Despite collecting numerous IP addresses of command-and-control servers, IDnS might still overlook parts of malware infections not reliant on domains. Furthermore, relying on administrators to supply specific IP addresses may not comprehensively address all potential threats.

2.11 A review of threat modelling approaches for APT-style attacks [15]

Several Machine Learning (ML) techniques were found to be used for threat categorization and prediction in our study. Notably, two articles using machine learning frameworks based on the tactics, techniques, and procedures (TTPs) of attackers were introduced by Noor et al. While the second paper assigns cyber risks to entities using TTPs, the first publication [19] proposes an ML framework inferring threat occurrences by evaluating the relationship between threats and TTPs. Furthermore, Farooq et al. [19] determined the most efficient method by analyzing, modeling, and assessing 11 ML algorithms against 4 ATT&CK Technique use scenarios. To maximize strengths and reduce weaknesses, the study recommends experimenting with different combinations of threat models.

Advantages:

The research offers a comprehensive analysis of different Machine Learning methods used for threat classification and prediction, providing insights into the methods' efficacy.

Disadvantages:

The study might only include a small number of specific machine learning techniques and threat scenarios, which could leave out new or innovative methods or dangers. The efficacy of the machine learning frameworks suggested by Noor et al. and the assessment carried out by Farooq et al. could be impacted by innate prejudices or presumptions, which would affect how broadly applicable the results are.

2.12 Discovering Suspicious APT Behaviors by Analyzing DNSActivities [20]

This study uses a deep neural network to efficiently exploit the connection between DNS activity and Advanced Persistent Threat.

The 6-layer fully connected neural network used in the deep learning technique for DNS behavior analysis is made up of layers that are made up of 7, 10, 8, 5, 3, and 1 neurons, respectively. The input data consists of serialized 8-dimensional feature vectors, from which a 7-dimensional vector is obtained by removing the first column, which shows the relationship between IP and domain. As a result, the input layer generates seven neurons. A one-dimensional label matrix with values closer to 1 denoting a higher suspicion of DNS activity is the intended output.

In order to optimize experimentation time, data pre-processing lowered the initial DNS request records from 4,907,147,146 to 376,605,606. Based on reports from BAE, Clearskysec, and Kaspersky Lab, 15,338 samples made up the black data, which mimicked APT strikes. One million innocent domain names from Alexa rankings made up the white data. Pre-processing of the grey data from Jilin University Education Online produced the final dataset. By employing a stacking method to reduce noise caused by oversampling in the training dataset, the experimental results were improved.

Advantages:

A full perspective of DNS traffic is provided by diverse datasets (black, white, and grey), which realistically capture both possible threats and benign operations.

Disadvantages:

Due to the difficulties in getting black data, oversampling in the training dataset may occur, which calls for the use of mitigation techniques like stacking.

2.13 Cyber Security Threat Intelligence Monitoring and Classification [16]

An intelligent detection system called DEST (Detect Remote Shell Threat) was created to examine risks to remote networks, specifically those that target SSH sessions. Data collection, data preprocessing, feature-based analysis, model training, and model output are the five primary parts of its architecture. The Cyberlab Honeypot dataset is the source of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

the dataset used for training and evaluation, guaranteeing a wide range of sample types. Preprocessing verifies the integrity of the data, and feature-based analysis assesses the relative significance of various feature combinations. In model training, the algorithm is trained and its performance is validated by benchmarking the predictions against those of previous studies.

The training and test datasets encompass data from 2019 and 2020, assessing the robustness of the proposed DEST system over time. The DEST classifier accurately predicts threat classifications in the test dataset, demonstrating consistent detection capabilities across varying attack periods and maintaining high efficiency and performance.

Advantages:

The system benefits from a rich feature set of 52 attributes, enhancing its threat comprehension. With an accuracy of 99.20% and an F1 score of 99.80%, it showcases superior performance. Its multi-dimensional approach bolsters detection accuracy across diverse attack types.

Disadvantages:

Implementation may be slowed considerably by the time and resources required for extensive preprocessing and feature extraction. Limited dataset diversity may cause issues for system performance and affect its efficacy under different threat scenarios. Continuous efforts are required to ensure that the system stays successful and flexible in addressing evolving threats through continual data collection and algorithm modification.

2.14 Understanding Awareness of Cyber Security Threat Among IT Employees [21]

The survey reveals a significant knowledge gap in cybersecurity awareness among IT employees, underscoring the importance of organizations prioritizing efforts to enhance employee knowledge and awareness in cybersecurity. To address this, we propose customizable assessment scenarios tailored to support organizations in staying updated with cybersecurity knowledge. The selection of the appropriate assessment type should be determined during the initial meeting, considering factors such as duration and the number of targets involved.

Network-Based Attack & Prevention: It's critical for enterprises to prevent network-based assaults such denialof-service attacks. In order to detect and reduce these risks, vulnerability assessments and penetration tests analyze the network's vulnerability to online threats, illegal access, and the efficiency of security measures.

Host-Based Assessment: Patching, service settings, and antivirus/malware protection are all evaluated when determining how secure workstations and servers are. Both manual inspections and automated scanning methods guarantee adherence to security best practices and spot locally exploitable vulnerabilities

Application Assessment: Examining an application's user and server interactions is necessary to determine its functionality and resiliency. By using scanning technologies and human testing to find vulnerabilities like SQL injection and cross-site scripting, this audit makes sure that data and services are protected.

Compliance: Ensuring adherence to legal standards is achieved by auditing systems for compliance with rules such as GDPR and HIPAA. Information security officers make sure that companies comply with regulations by organizing audits or verifying compliance.

Physical Security Assessment: To ensure the safety of computer resources, physical and environmental controls are evaluated through interviews, documentation reviews, and on-site visits. In order to preserve the security of vital computing infrastructure, evaluations concentrate on environmental sustainability and physical access controls.

Advantages:

Through assessment-based identification of vulnerabilities, weaknesses, and compliance gaps, companies can enhance their entire security posture and proactively manage risks. This proactive strategy aids in averting possible data and security breaches.

Disadvantages:

Organizations may become overwhelmed by the amount of data and conclusions generated by assessments, especially if they lack the knowledge or resources necessary to properly prioritize and analyze the results. The amount of information available could cause delays in resolving urgent security concerns.

Although assessments are useful in identifying vulnerabilities and weaknesses that already exist, they might not be able to predict new threats or stop security problems in the future. Without properly planning for potential hazards in the future, organizations risk being mired in a reactive loop of resolving difficulties as they arise.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

2.15 A Comprehensive Overview on Cybersecurity: Threats and Attacks [22]

Scholars put forth a variety of approaches to tackle cybersecurity issues. A quantitative approach using a Bayesian network (BN) is proposed by Żebrowski, Couce-Vieira, and Mancuso (2022) to provide an allencompassing perspective of cybersecurity vulnerabilities and evaluate different attack scenarios. Their BNintegrated multiobjective optimization technique helps create complex security objectives. A strategy for managing cyber risk that stresses ongoing development in line with changing data protection laws is presented by Lee (2020). This method emphasizes how crucial it is to incorporate organizational risk management procedures with cybersecurity initiatives. Using qualitative analysis of secondary data, Baby and Nirmaladevi (2022) investigate the effectiveness of data mining approaches in cybersecurity with regard to data gathering strategies. Salem et al. (2022) emphasizes the use of data mining in auditing and intrusion detection for national security.

Advantages:

A more comprehensive understanding of cybersecurity flaws and attack scenarios is provided by the suggested approaches, which improve risk assessment.

Frameworks such as the one Lee (2020) outlines make it easier for organizations to comply with changing data protection laws.

As demonstrated by Baby and Nirmaladevi (2022) and Salem et al. (2022), the application of data mining techniques facilitates the efficient identification of malware and intrusions, hence augmenting cybersecurity.

Disadvantages:

The availability and quality of data, which can be difficult to come by, especially for real-time applications, are prerequisites for the efficacy of data mining techniques. Organizations may have to incur additional administrative expenses and responsibilities in order to comply with changing data protection requirements, which could hinder the implementation of cybersecurity strategies.

IV. ANALYSIS TABLE

The following table gives the analysis of techniques and methods used in research papers on APT detection and identification.

Sr No	Paper Title	Authors	Method
1	A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model	Duraid Thamer Salim et.al	Pattern matching based detection, anomaly-based detection, Clustering technique, Ensemble learning, SVM, Linear regression
2	APT Beaconing Detection: A Systematic Review	Manar Abu Talib et.al	Signature-based detection, Network flow analysis-based detection, The graph-based anomaly detection method, A game-based method.
3	An Approach for Detection of Advanced Persistent Threat Attacks	Qingtian Zou et.al	APT Repository: Contains predefined APT strategies and techniques. APT Technique Identifiers: Used to identify specific techniques employed in APT attacks. APT Matcher: Matches identified APT approaches to the strategies stored in the APT repository. APT Ranker: Ranks APT instances based on their completeness.
4	Advanced Persistent Threat Identification with Boosting and Explainable AI	Md. Mahadi Hasan et.al	Boosting Algorithms: AdaBoost, Gradient Boosting.
5	A novel approach for detecting	Jaafer Al-Saraireh	Classification algorithms, Decision trees, random

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

	advanced persistent threats	and Ala Masarweh	forests, support vector machines (SVM), or gradient boosting machines
6	Locate-Then-Detect: Realtime Web Attack Detection via Attention-based Deep Neural Networks	Tianlong Liu et.al	Payload Locating Network (PLN), Payload Classification Network (PCN), Web Attack Annotation , Locate-Then Detect (LTD) Mechanism
7	Web-APT-Detect: A Framework For Web-Based Advanced Persistent Threat Detection Using Self Translation Machine with Attention	Liu Yan and JayXiong	Anomaly Detection, neural network based approaches.
8	Comprehensive Detection Method for the Lateral Movement Stage of APT Attacks	Daojing He et.al	Deep learning frameworks like TensorFlow.
9	A novel approach for APT attack detection based on combined deep learning model	Cho Do Xuan and Mai Hoang Dao	deep learning-based feature extraction techniques like CNN, MLP, and LSTM and IP categorization techniques
10	Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis	Guodong Zhao and KE XU	Malicious DNS Detector Classifier, J48 decision tree algorithm, based on the C4.5 algorithm.

V. CONCLUSION

The study conducted a comprehensive literature review of several articles published between 2015 and 2023 to explore the landscape of Advanced Persistent Threat (APT) malware detection techniques. It revealed that machine learning (ML) methods dominate the field, with clustering, extreme learning, random forest, decision tree, and various others being extensively utilized. However, traditional intrusion detection systems (IDSs) were found ineffective in real-time APT malware detection due to the dynamic nature of APT behaviors. While some studies experimented with security analytics (SA) models to monitor and analyse network traffic for APT detection, traditional IDSs continue to face challenges in this aspect.

A few publications employed CSA models for network traffic analysis and monitoring in order to identify APT malware utilizing SA models. We draw the conclusion that identifying APT malware through network traffic analysis and monitoring remains a problem for typical intrusion detection systems.

To mitigate the challenge IDSs faces, we suggest a technique that combines supervised learning for threat detection and unsupervised learning for anomaly detection in identifying Advanced Persistent Threats (APTs). Supervised models like SVMs or RF are trained on labeled data to classify malicious and benign activities, while unsupervised methods detect anomalies in system behavior or network traffic without predefined labels, enhancing proactive threat identification.

Unsupervised learning techniques like clustering or anomaly detection algorithms, such as Isolation Forest or Autoencoders, are employed for anomaly detection, requiring no labeled data. These methods detect deviations from normal behavior in system or network traffic, flagging suspicious activities indicative of APTs. By combining supervised and unsupervised learning, the technique enhances APT detection by leveraging both labeled and unlabeled data to identify and mitigate threats effectively.

REFERENCES

[1]. Salim DT, Singh MM, Keikhosrokiani P. A systematic literature review for APT detection and effective cyber situational awareness (ECSA) conceptual model. Heliyon. 2023 Jun 16.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

[2]. Talib MA, Nasir Q, Nassif AB, Mokhamed T, Ahmed N, Mahfood B. APT beaconing detection: A systematic review. Computers & Security. 2022 Aug 21:102875.

[3]. Zou Q, Sun X, Liu P, Singhal A. An approach for detection of advanced persistent threat attacks. Computer. 2020 Dec 1;53(12):92-6.

[4]. Hasan MM, Islam MU, Uddin J. Advanced Persistent Threat Identification with Boosting and Explainable AI. SN Computer Science. 2023 Mar 20;4(3):271.

[5]. Al-Saraireh J. A novel approach for detecting advanced persistent threats. Egyptian Informatics Journal. 2022 Dec 1;23(4):45-55.

[6]. Liu T, Qi Y, Shi L, Yan J. Locate-Then-Detect: Real-time Web Attack Detection via Attention-based Deep Neural Networks. InIJCAI 2019 Aug 10 (pp. 4725-4731).

[7]. Yan L, Xiong J. Web-APT-Detect: a framework for web-based advanced persistent threat detection using self-translation machine with attention. IEEE Letters of the Computer Society. 2020 Jun 1;3(2):66-9.

[8]. He D, Gu H, Zhu S, Chan S, Guizani M. A comprehensive detection method for the lateral movement stage of apt attacks. IEEE Internet of Things Journal. 2023 Oct 6.

[9]. Do Xuan C, Dao MH. A novel approach for APT attack detection based on combined deep learning model. Neural Computing and Applications. 2021 Oct;33:13251-64.

[10]. Zhao G, Xu K, Xu L, Wu B. Detecting APT malware infections based on malicious DNS and traffic analysis. IEEE access. 2015 Jul 20;3:1132-42.

[11]. Chu WL, Lin CJ, Chang KN. Detection and classification of advanced persistent threats and attacks using the support vector machine. Applied Sciences. 2019 Oct 28;9(21):4579.

[12]. Xiong C, Zhu T, Dong W, Ruan L, Yang R, Cheng Y, Chen Y, Cheng S, Chen X. CONAN: A practical real-time APT detection system with high accuracy and efficiency. IEEE Transactions on Dependable and Secure Computing. 2020 Feb 3;19(1):551-65..

[13]. J. Straub, "Modeling attack, defense and threat trees and the cyber kill chain, att&ck and stride frameworks as blackboard architecture networks," in 2020 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, 2020, pp. 148–153.

[14]. W. Tian, M. Du, X. Ji, G. Liu, Y. Dai, and Z. Han, "Honeypot detection strategy against advanced persistent threats in industrial internet of things: a prospect theoretic game," IEEE Internet of Things Journal, vol. 8, no. 24, pp. 17372–17381, 2021.

[15]. M. Tatam, B. Shanmugam, S. Azam, and K. Kannoorpatti, "A review of threat modelling approaches for apt-style attacks," Heliyon, vol. 7, no. 1, 2021.

[16]. Wang BX, Chen JL, Yu CL. Cyber security threat intelligence monitoring and classification. In2021 IEEE International Conference on Intelligence and Security Informatics (ISI) 2021 Nov 2 (pp. 1-3). IEEE.

[17]. J. Straub, "Modeling attack, defense and threat trees and the cyber kill chain, att&ck and stride frameworks as blackboard architecture networks," in 2020 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, 2020, pp. 148–153.

[18]. Jiazhong Lu, Chen K, Zhuo Z, Zhang XS (2019) A temporal correlation and traffic analysis approach for APT attacks detec tion. Clust Comput 22:7347–7358

[19]. U. Noor, A machine learning framework for investigating data breaches based on semantic analysis of adversary's attack patterns in threat intelligence repositories, Future Generat. Comput. Syst. 95 (2019) 467–487.

[20]. Yan G, Li Q, Guo D, Meng X. Discovering suspicious APT behaviors by analyzing DNS activities. Sensors. 2020 Jan 28;20(3):731.

[21]. Al-Mohannadi H, Awan I, Al Hamar J, Al Hamar Y, Shah M, Musa A. Understanding awareness of cyber security threat among IT employees. In2018 6th international conference on future internet of things and cloud workshops (ficloudw) 2018 Aug 6 (pp. 188192). IEEE.

[22]. Abrahams TO, Ewuga SK, Dawodu SO, Adegbite AO, Hassan AO. A Review Of Cybersecurity Strategies In Modern Organizations: Examining The Evolution And Effectiveness Of Cybersecurity Measures For Data Protection. Computer Science & IT Research Journal. 2024 Jan 9;5(1):1-25.