Pegem Journal of Education and Instruction, Vol. 13, No. 3 , 2023 (pp. 430-439)

RESEARCH ARTICLE WWW.PEGEGOG.NET

A Natural Language Processing-Based System for Automatically Identifying and Profiling New Cyber Threats

[1]Mrs. T. KAVITHA, [2]M. SRAVANTHI, [3]M. PUJITHA, [4]B. KEERTHANA

[1]Assistant Professor, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India
Email: kavitha.tirunagiri@gmail.com
[2,3,4,]B.Tech Student, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India

ABSTRACT

More and more, the amount of time that elapses between the discovery of a new cyber vulnerability and its exploitation by cybercriminals is shrinking. This is well shown by recent incidents, such the Log4j vulnerability. Attackers began searching the web for sites that could be susceptible to the exploit in order to install malware such as bit coin minersand ransom ware on those servers within hours of the vulnerability's announcement. For this reason, early threat and capability detection is crucial for cyber security defence strategies in order to maximize the efficacy of preventative measures. Finding new threats is an important but difficult task for security analysts since there is a mountain of data and information sources that need to be sifted through for indications of a developing danger. To that end, we provide a system that can automatically detect and profile new threats based on their characteristics, with MITRE ATT&CK serving as a database of threat information and Twitter posts as an event source. The three primary components of the framework are as follows: first, the naming and classification of cyber threats; second, the use of two machine learning layers to filter and categories tweets in order to profile the detected danger according to its aims or goals; and third, the creation of alarms depending on the risk posed by the threat. Our method to identifying dangers and characterizing them based on their intents or aims provides extra information and potential mitigation strategies. Our trials showed that the profiling step was able to accurately profile 77% of the threats that were found.

Keywords: Cyber Threats

INTRODUCTION

Since the advent of hyper-connectivity and hyper mobility, people have grown to depend more and more on the Internet for their personal, professional, and societal lives. Despite the Internet's growing importance as a social, political, and economic

Corresponding Author e-mail: kavitha.tirunagiri@gmail.com
How to cite this article: 1Mrs. T. KAVITHA, 2M. SRAVANTHI, 3M. PUJITHA, 4B. KEERTHANA. Naveena A Natural Language Processing-Based System for Automatically Identifying and Profiling New Cyber Threats.Pegem Journal of Education and Instruction, Vol. 13, No. 3, 2023, 430-439
Source of support: Nil **Conflicts of Interest:** None.
DOI: 10.48047pegegog.13.03.44
Received: 12.09.2023
Accepted: 22.10.2023 **Published:** 24.11.2023

infrastructure, there is a growing anger of cyber assaults driven by a variety of hostile actors. Organizations need upto-date information on cyber vulnerabilities and assaults, sometimes called threats, in order to protect themselves against cyber exploits. "Status, methods, indicators, implications, and practical guidance based on evidence concerning a current or future danger to assets that can be utilized to guide decisions concerning the subject's reaction to that danger" is what threat intelligence is said to be.

The purpose of cyber threat intelligence is to assist detect possible security vulnerabilities and attacks more accurately by providing up-to-date and relevant information, such as attack signatures. Informal and formal sources, which formally disseminate threat information in structured data format, are the usual go-to places for cyber threat intelligence extraction. When it comes to structured threat intelligence, consistency in format and organization is key. In order to assess and react to security risks appropriately, security technologies can simply interpret structured cyber threat information. Some examples of official cyber threat intelligence sources include the 1 and the Common Vulnerabilities and Exposures (CVE) database. Page 4, 2023 of the CVSS database 1 It has been decided that this piece will be published in IEEE Access. Since this is the author's work in progress, it may undergo revisions before publication. This work is referenced as DOI 10.1109/ACCESS.2023.3260020. The Attribution-Noncommercial-No Derivatives 4.0 Licence is the legal framework under which this work is housed. Article Authors and Others: IEEE Transactions and Journals Paper Preparation The National Vulnerability Database (NVD) No. 2. Informal sources of cyber threat intelligence include public forums, social media, dark webs, blogs, and public blogs. In real-time, any Internet user or organization may post danger information in an unstructured data format or using natural language via informal sources. Open Source information Network (OSINT) is another name for the publicly accessible, unstructured threat information. For cyber security events like security vulnerability exploitation, OSINT that is relevant to cyber security may serve as an early warningsystem. First, cybercriminals must find security holes; second, they must gather the skills and resources to exploit those holes; third, they must choose a target and enlist accomplices; fourth, they must

build or buy the infrastructure required to launch the assault; and last, they must organize and carry out the operation. There may be vulnerability discussions or attack response coordination including other players, such as victims, security analysts, and system administrators. By engaging in these pursuits online— in places like social media, (public and private) online forums, and professional blogs—participants typically leave digital footprints. When added together, these digital footprints provide important information about the ever-changing nature of cyber threats and may alert the user to an impending or ongoing assault before any harmful actions are detected on the target system. By way of illustration, Twitter is where exploits are discussed before to their public disclosure, and dark web forums even precede social media discussions about them.

RELATED WORK

Identification and tracking of very clandestine, unidentified cyber threats

At this pivotal juncture, the strategic defence concept of "active defence, traceability, and countermeasures" emerges in response to the growing severity of network security threats and the emergence of advanced persistent threats (APTs), making cyberspace threat intelligence (CTI) an invaluable tool for strengthening defences against cyberattacks. In response to the real need for APT defence, we developed a new automation system, CTI View, that uses the processing of natural languages to process cyberspace threat intelligence (CTI). This system is focused on extracting and analysing text from the vast amounts of unstructured CTI that security vendors release. The following is the core functionality of CTI View: (1) using an automated testing framework, text recognition technology, and text demising technology, a threat intelligence text extraction framework is developed to handle diverse CTI. It efficiently addresses the issue of limited flexibility while crawling diverse CTI using crawlers; (2) extracting the IOC and TTP information from CTI using regularexpressions and a blacklist/whitelist mechanism; (3) making use of a model based on bidirectional encoder representations from transformers (BERT) to finish the entity extraction algorithm for heterogeneous threat intelligence according to the actual requirements.

In this study, we enhance the BERTBLits-CRF model by adding a GRU layer. We then test this model on the marked dataset and find that it outperforms the current

popular entity extraction method.

Synopsis of threat intelligence sharing and exchange in network security .

With their sophisticated and ever- evolving assault techniques, new cyber dangers are putting the interests of people, businesses, and governments at risk. Cyberspace security has reason to be hopeful thanks to the threat information sharing and exchange system, which steps in when more conventional methods of network security defence are inadequate. Originations and institutions may be harmed in indirect or direct ways by the information that makes up cyber security threat intelligence. With this data, institutions and businesses may better assess the cyber security risks they confront, plan responses, and implement policies. Improving threat detection and emergency response capabilities for all parties concerned is possible via the exchange and sharing of threat intelligence, which may maximize the value of threat intelligence, minimize the cost of intelligence search, and relieve the issue of information islands. After defining cyber threat intelligence and outlining generally accepted practices for sharing such information, the article delves into the literature on the topic over the last decade, both domestically and internationally, before concluding with an analysis and summary of the state of the art and future directions for such exchanges. Examining sharing models and processes, exchanging advantages, and protecting shared data from prying eyes are the three main points of this article's examination. We highlight the issues in all three sections and provide potential remedies; we then evaluate and analyze the pros and cons of each option. Lastly, we look forward to the direction and trend of future research on threat intelligence exchange and sharing.Automated learning of harmful campaign semantics by threat intelligence report mining: Chain Smith

Commonly carried out as part of bigger efforts, modern cyberattacks follow a certain protocol. One way to quantify these initiatives is via large- scale field data. Comparatively, security professionals manually extract and report qualitative campaign characteristics. New insights into attacker techniques from measurements are provided by linking the two sources. Nevertheless, this endeavour is laborious due to the fact that machine readability is not often a feature of qualitative data presented in natural language. A method to integrate measurement data with human analysis is shown here. We take a page out of threat intelligence's playbook: characterize each step of a campaign using indications of compromise (IOCs), such as URLs and IP addresses. We then use this model

to design campaigns. We learn to use a multi-class classifier to separate IOCs into their respective phases. Chain Smith is the mechanism that we use to put these principles into action. We are able to extract IOCs with a 91.9% accuracy rate and a 97.8% recall rate, and we can identify the campaign roles for 86.2% of IOCs with a 78.2% accuracy rate and an 80.7% recall rate..Our analysis of 14,155 web security publications yields 24,653 IOCs. With the use of semantic roles, we may connect manual attack analysis with field measurements taken on a broad scale. In specifically, we investigate how various persuasive strategies work to get users to download the payloads. It turns out that social engineering is where most campaigns begin, and that the "missing codec" scam is a popular way to get people to download questionable files. **One method for automatically obtaining threat intelligence from unstructured sources is to use supervised machine learning.**

Shared Cyber Threat Intelligence (CTI) has been on the rise, signalling a paradigm change in cyber protection strategies from reactive to proactive in recent years. Many different analytical systems now take their threat feeds from the many Open Source Intelligence (OSINT) sources that are constantly updating their databases.

Both organised (STIX, Opinion, etc.) and unstructured (blacklists, etc.) datais now flying out of these kinds of sources. A lot of the time, however, threat feeds lack the granularity needed to make educated security judgments since most indications are atomic in nature, such as IP addresses and hashes, which may be quite unpredictable. These feeds severely deficiency in strategic threat data, such as assault patterns and methodologies that accurately depict an attacker's or exploit's conduct. Additionally, there is a great deal of duplicate threat information and no central location to investigate a danger in its completeness, thus it takes a lot of time and effort (hundreds of man-hours) to uncover all the trustworthy information on a threat by sorting through several sources (trying to separate signal from noise). Utilizing natural language processing, we have extracted threat feeds from unstructured cyber threat information sources with a precision of around 70%. Our complete threat reports are formatted according to industry standards such as STIX, which stands

for CTI and is often accepted. The timely collecting and sharing of important CTI would offer organizations the advantage to proactively protect against known and undiscovered dangers, and automation of an otherwise arduous human operation would make this possible.

METHODOLOGY

We have developed the following modules to fulfil this project's requirements.

1) Using this module, we will upload the APT attack dataset to the programme. We will then search the dataset for cyber security assaults and produce a graph with the names and frequencies of each attack. 2) Dataset-Generated Knowledge Graph: This module allows us to enter the complete dataset into a graph algorithm, which then builds a knowledge graph. The graph then shows how attackers use network properties.

3) Preprocess Dataset: with the help of this module, we will eliminate any missing values, shuffle and normalize the dataset, and divide it into two parts: the train set, which the deep learning algorithm will use for training, and the test set, which it will use for testing.

4) Execute BI-LSTM with GRU

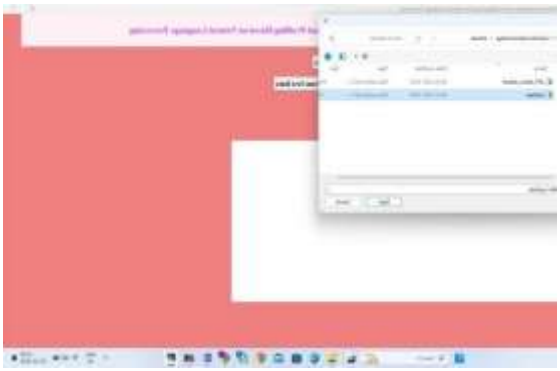
Algorithm: The 80% dataset will be fed into the BI-LSTM algorithm to train a model, which will then be tested on test data to determine the accuracy

of-the-predictions.

5) Graph for Comparison: We will use this module to create a graph for comparing criteria like proposed algorithm-accuracy. 6) Attack Detection from Test Data: This module allows us to submit test data and use an algorithm to assess it in order to forecast APT assaults.

RESULTS

All of the algorithmic metrics are approaching 1, as seen in the following graph, which uses the x-axis to show names of deep learning BI-LSTM measures like accuracy and the y-axis to show values. After you've closed the previous graph, you can see that this method performs the best. To upload test data and get threat prediction output, click the "Attack Detection from Test Data" button.



In above screen we are selecting and uploading ‘testData.csv’ file and then click on ‘Open’ button to get below output

In above screen in blue color text we can see predicted APT as ‘Hurricane’ and similarly scroll down above screen to view all threats

In above screen in square bracket we can see test data and after arrow symbol =➒ we can see predicted Threat which is showing in below screen

CONCLUSION

The KCTIAA tool for automated network threat intelligence analysis is proposed in this study. KCTIAA strengthens the pre-trained model's grasp of cyber security jargon by including the cyber security knowledge graph. For the purpose of knowledge fusion of pre-trained models, K-CTIAA suggests two novel and enhanced approaches. Furthermore, K-CTIAA may assist network security professionals in dealing with a variety of network security challenges by finding information about threat actors and providing matching threat behavior countermeasures based on the relevant knowledge of the network security knowledge graph. According to the findings of the experiments, K-CTIAA is the best approach.

REFERENCES

[1] Advanced Persistent Threat, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Advanced_persistent_threatInformati on and communication technology.

[2] APT Annual Review, 2021. [Online]. Available: https://securelist.com/apt-annual-review-2021/105127

[3] T.Zigong, "Detection and traceability of high covert unknown threats in cyberspace," Inf. Communed. Technol., vol. 14, no. 06, pp. 4–7, 2020.

[4] L.Yuen , “Overview of network security threat intelligence sharing and exchange,” Compote. Res. Develop., vol. 57, no. 10, pp. 2052–2065, 2020.

[5] Z. Zhu and T. Dmitri’s, “Chain Smith: Automatically learning the semantics of malicious campaigns by mining threat intelligence reports,” in Proc. IEEE Eur. Sump. Secure.
Privacy, 2018, pp. 458–472.

[6] Y. Ghazi, Z. Anwar, R. Mutes, S. Salem, and A. Tahir, “A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources,” in Proc. Int. Conf. Front. Inf.
Technol., 2018, pp. 129–134.

[7] Y. Zhao, B. Lang, and M. Liu, “‘Ontology-based unified model for heterogeneous threat intelligence integration and sharing,” in Proc. 11th IEEE Int. Conf. Anti-Counterfeiting Secure. Identification, 2017, pp. 11–15.

[8] Y.Goo, “CyberReel: Joint entity and relation extraction for cyber security concepts,” in Proc. Int. Conf. Inf. communed. Secured. 2021, pp. 447–
463.

[9] G.Hussar, E. Al-Shear, M. Ahmed, B. Chu, and X. Nia, “TTPDrill: Automatic and accurate extraction of threat actions from unstructured text ofCTI Sources,” in Proc. 33rd Annu. Compute. Secured. Appl. Conf., 2017, pp. 103–115.

[10] Z. Li, J. Zeng, Y. Chen, and Z. Liang, “Attack: Constructing technique knowledge graph from cyber threat intelligence reports,” 2021, areXiv:
2111.07093.