Automated Emerging Cyber Threat Identification and Profiting based on Natural Language Processing

Koppadi Pavan Kumar[1], Mr. Sesha Giri Rao Thalluri[2]
[1]*PG Scholar, Dept of CSE, Bonam Venkata Chalamayya Engineering College, Odalarevu*
[2]*Associate Professor, Dept of CSE, Bonam Venkata Chalamayya Engineering College, Odalarevu*

Abstract: ***The duration of time window between the disclosures of new recent scenarios The Log4j vulnerability was identified in more, host to deployed threat in the target system. Within hours after the exploit was released attacker started scanning the network looking for vulnerability host to deploy threads like ransom ware crypto currency miners etc on the systems. When attacker started scanning the internet looking for vulnerable cyber vulnerability used by the cyber criminals, has been getting very smaller overtime. It becomes imperative for the cyber security defence strategy to detect threats and their capabilities as early as possible to minimize success of prevention action all though crucial discovering new threats is a challenging activity for security analysis due to the immense volume of data and information sources to analyse for signs that a threat is emerging. The framework comprises three main parts identification of cyber threats, profile in the identified threat and alarm generation based on threats risk. Represent a framework for automatic identification and profiling of emerging threads using social media messages as a source of events and MITRE attack as a source of knowledge for thread classification. The main contribution of our work is the approach to classifying and identifying threats in terms of their intentions and providing additional context on the threat for mitigation.***

Keywords: ***vulnerability, disclosures, intentions, comprises, exploit, Log4j, capabilities, prevention, ransom ware, immense, scanning, framework, defence, strategy, discovering.***

I. INTRODUCTION

In today's scenario interconnected world cyber security has become one of the most pressing challenges facing organisations governments and individuals. As technology evolves, there is more situations to sophisticate of cyber threads the traditional methods of detecting and responding to cyber attacks are often reactive, relaying on indicators of compromise that is IOC's or historical attack patterns. However the rapid pace of cyber crime innovation means that emerging threads are increasingly difficult to predict and detect before the cause significant harm. To identify these attacksIn the growing world Artificial Intelligence(AI) specifically Natural Language Processing(NLP) to automatic the identification and understanding of emerging cyber threats.NLP focused on the interaction between computers and human language offers and innovative approach to monitoring and identifying cyber threads at scale by analysing vaaste amount of unstructured data like reports social media posts dark web communication and security block and NLP extract valuable inside that would be consuming are impossible for human analysis to detect manually.

Automatic amazing cyber threat identification leverages the capabilities of NLP to detect, analyse and to predict the cyber threats before the fully materialized. By processing large volume of unstructured data such as social media posts articles in the news forum discussions and event dark web communication NLP models can identify early indicators of new and evolving cyber attacks this approach enable cyber security professional to stay ahead of potential threats mitigate risk before they escalate and allocate resources more efficiently. The value of threat intelligence is not just in identifying emerging risks but also monetizing these types of scenarios.

The ability of anticipate cyber threads of a significant business opportunities the organisations are willing to pay a premium for timely actionable information that can help them protect their system data and other asset by integrating threat intelligence platform with real time NLP based analysis business in create some fusion models offer consulting services. The coverage of automated emerging cyber security threat identification and nlp presence a unique opportunity for innovation in both and cyber security and business these paper explores the use of an lp for

automated emerging cyber threat identification outlines various methods for monetizing this intelligence and discuss the partial implications challenges and potential rewards of this innovative approach to cyber security.

II. LITERATURE SURVEY

The profusion of unstructured data forced organizations to manage and take advantage of such data especially in the decision making process. The feasibility of integrating or mapping unstructured data to a data warehouse is becoming significant to bridge this gap and take the full potential of these data.

Data is the lifeblood of any organization. In today's world, organizations recognize the vital role of data in modern business intelligence systems for making meaningful decisions and staying competitive in the field. Efficient and optimal data analytics provides a competitive edge to its performance and services. Major organizations generate, collect and process vast amounts of data, falling under the category of big data. Managing and analyzing the sheer volume and variety of big data is a cumbersome process. At the same time, proper utilization of the vast collection of an organization's information can generate meaningful insights into business tactics. In this regard, two of the popular data management systems in the area of big data analytics (i.e., data warehouse and data lake) act as platforms to accumulate the big data generated and used by organizations. Although seemingly similar, both of them differ in terms of their characteristics and applications.

III. SYSTEM ANALYSIS

Existing System

Cyber security is becoming an ever increasing concern for most organizations and much research has been developed in this field over the last few years. Inside these organizations, the Security Operations Center (SOC) is the central nervous system that provides the necessary security against cyber threats. However, to be effective, the SOC requires timely and relevant threat intelligence to accurately and properly monitor, maintain, and secure an IT infrastructure. This leads security analysts to strive for threat awareness by collecting and reading various information feeds. However, if done manually, this results in a tedious and extensive task that may result in little knowledge being obtained given the large amounts of irrelevant information. Research has shown that Open Source Intelligence (OSINT) provides useful information to identify emerging cyber threats. OSINT is the collection, analysis, and use of data from openly available sources for intelligence purposes [7]. Examples of sources for OSINT are public blogs, dark and deep websites, forums, and social media. In such platforms, any person or entity on the Internet can publish, in real time, information in natural language related to cyber security, including incidents, new threats, and vulnerabilities. Among the OSINT sources for cyber threat intelligence, we can highlight the social media Twitter as one of the most representative [8]. Cyber security experts, system administrators, and hackers constantly use Twitter to discuss technical details about cyber attacks and share their experiences [4].

Utilization of OSINT to automatically identify cyber threats via social media, forums and other openly available sources using text analytics was proposed in different researches. However, most proposals focus on identifying important events related to cyber threats or vulnerabilities but do not propose identifying and profiling cyber threats. Amongst research, proposes an early cyber threat warning system that mines online chatter from cyber actors on social media, security blogs, and dark web forums to identify words that signal potential cyber-attacks. The framework is comprised by woman in components: text mining and warning generation. The text mining phase consist son pre-processing the input data to identify potential threat names by discarding 'known'' terms and selecting repeating 'unknown'' among different sources as they potentially can be the name of a new or discovered cyber threat. The second component, warning generation, irresponsible for issuing alarms for unknown terms that meet some requirements, like appearing twice in a given period of time. The approach presented in this research uses keyword filtering as the only strategy to identify cyber threat names, which may result in false positives as unknown words may appear in tweets or other content not necessarily related to cyber security. Additionally, this research does not profile the identified cyber threat. First, the proposed approach does not name the identified threat. Naming the threat is an important step to cyber threat

intelligence as it may allow analysts to identify and mitigate campaigns based on the historic modus operandi employed by a given threat or group. Second, the proposed approach relies on an external component to classify tweets as related or not to cyber security as opposed to our approach that proposes a component to classify tweets using machine learning trained with the evolving knowledge from MITRE ATTACK. Third, instead of using a keyword match to pre-filter threats and a fixed list of threat types, we present an approach to profile the identified cyber threat to spot in which phase of phases of the cyber kill chain the given threat operates in. This is important for a cyber threat analyst as he or she may employ the necessary mitigation steps depending on the threat profile.

Disadvantages

An existing system never implemented Multi-Class machine learning (ML) algorithms – the next An existing system didn't implement(steps in the pipeline. The following method process identified and classified threats.

Proposed System:

The overall goal of this works to propose an approach to automatically identify and profile emerging cyber threats based on OSINT (Open Source Intelligence) in order to generate timely alerts to cyber security engineers. To achieve this goal, we propose a solution whose macro steps are listed below.

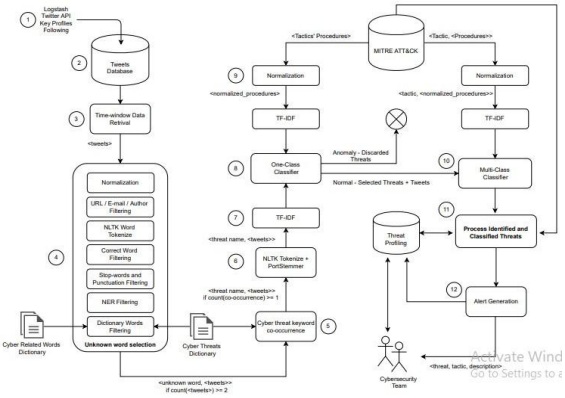
1) Continuously monitoring and collecting posts from prominent people and companies on Twitter to mine unknown terms related to cyber threats and malicious campaigns;
2) Using Natural Language Processing (NLP) and Machine Learning (ML) to identify those terms most likely to be threat names and discard those least likely;
3) Leveraging MITRE ATTACK techniques' procedures examples to identify most likely tactic employed by the discovered threat.
4) Generating timely alerts for new or developing threats along with its characterization or goals associated with a risk rate based on how fast the threat is evolving since its identification.

Advantages

To conduct a cyber-attack, malicious actors typically have to

1) Identify vulnerabilities
2) Acquire the necessary tools and tradecraft to successfully exploit them,
3) Choose a target and recruit participants
4) Create or purchase the infrastructure needed, and
5) Plan and execute the attack. Other actors— system administrators, security analysts, and even victims— may discuss vulnerabilities or coordinate a response to attacks.

IV. SYSTEM ARCHITECTURE



Cyber security threat detection using data from Twitter and the mitre attack framework the components are

1. Data sources: which database collects from logs dash Twitter API key profiles and user interactions mitre attack framework provides information on tactics and procedures from cyber threads.
2. Processing and normalisation: the data is retrieved within a time window and undergoes various filtering techniques like email other filtering word normalisation etc dictionary based filtering is used to select relevant words from the cyber related words dictionary if tweet contains two or more unknown words it is further analysed.
3. Future extraction and classification: TF-IDF (Term Frequency Inverse Document Frequency) extracts important terms from twit and mitre attack procedures one class classifier identify the normalise and disguise and relevant threads multi class classifiers classifies identity threads
4. Thread profiling: threat are identified classified and processed using a dictionary of cyber threads and natural language processing techniques thread profiling determines if a

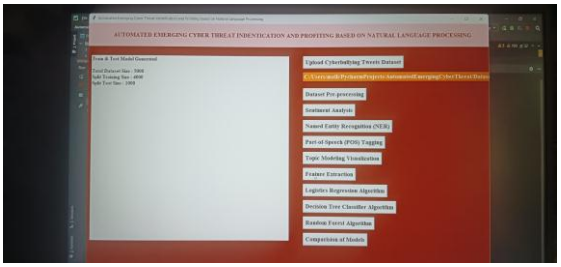
keyword is related to an actual cyber threat

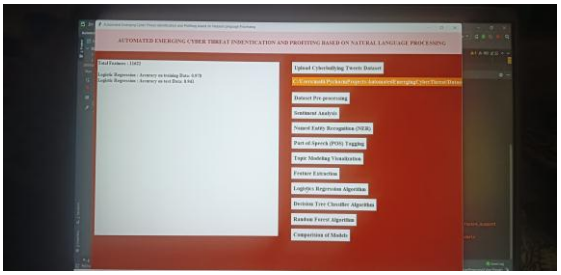
5. Output and Alert Generation: classified threats are presented to cyber security team alerts are generated based on threats detected.

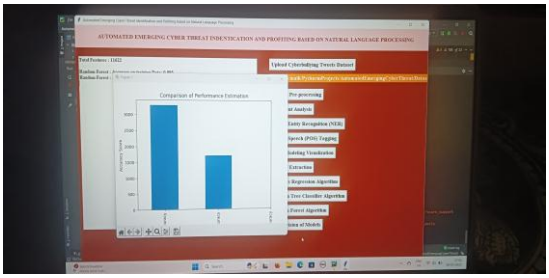
V. DISCUSSION

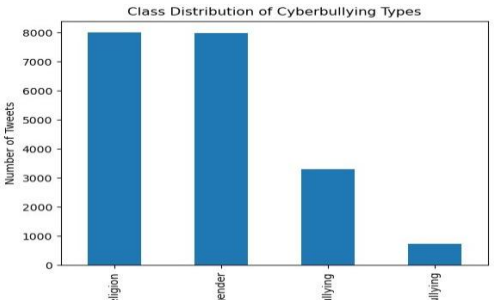
The existing cyber security release and Open Source Intelligence(OSMT) to detect threads but legs multiple class mission learning for effective classification manual threat analysis is tedious and initiate leading to potential intelligence gaps the proposers system and hands OSMT based detection using NLP and ml to continuously mounting Twitter for emerging threads integrates MIRE ATT&CK to classify threats based on attack tactics improving accuracy existing approaches it profile that is the cyber kill chain to support mitigation by automatic threat identification and classification the system provide timely alerts helps cyber security analysts to respond proactively to evolving cyber threat.

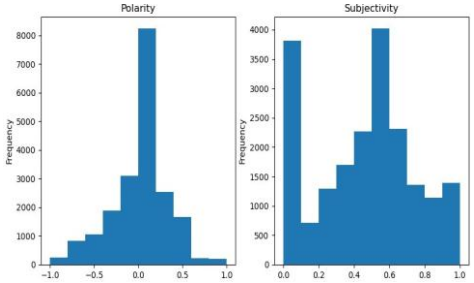
VI. RESULT











VII. CONCLUSION

Vulnerabilities and threats appearing at any time, keeping up to date on them is a challenging but important task for analysts. Even following the best practices and applying the best controls, a new threat may bring an unusual way to subvert the defences requiring a quick response. This way, timely information about emerging cyber threats becomes paramount to a complete cyber security system. This research proposes an automated cyber threat identification and profiling based on the natural language processing of Twitter messages. The objective is exactly to cooperate with the hard work of following the rich source of information that is Twitter to extract valuable information about emerging threats in a timely manner. This work differentiates itself from others by going a step beyond identifying the threat. It seeks to identify the goals of the threat by mapping the text from tweets to the procedures conducted by real threats described in MITRE ATT&CK knowledge base. Taking advantage of this evolving and collaborative knowledge base to train machine learning algorithms is a way to leverage the efforts of cyber security community to automatically profile identified cyber threats in terms of their intents. To put in test our approach, in addition to the research experiment, we implemented the proposed pipeline and run it for 70 days generating online alerts for the Threat Intelligence Team of a big financial institution in Brazil. During this period, at least three threats made the team take preventive actions, such as the PetitPotam case, described in section V.

Our system alerted the team making them aware of PetitPotam 17 days before the official patch was published by Microsoft. Within this period, the defence team was able to implement mitigations avoiding potential exploits and, consequently, incidents. Our experiments showed that the profiling stage reached an F1 score of 77% in correctly profiling discovered threats among 14 different tactics and the percentage of false alerts of 15%.

VII. REFERENCE

[1] Ba Dung Le, Guanhua Wang, Mehwish Nasim, and Ali Babar. Gathering cyber threat intelligence from twitter using novelty classification. arXiv preprint arXiv:1907.01755, 2019.

[2] Gartner Research. Definition: Threat intelligence, 2013.

[3] Robert David Steele. Open source intelligence: What is it? why is it important to the military? American Intelligence Journal, pages 35–41, 1996.

[4] Carl Sabottke, Octavian Suciu, and Tudor Dumitras, . Vulnerability disclosure in the age of social media: Exploiting twitter for predicting real-world exploits. In 24th {USENIX} Security Symposium ({USENIX} Security 15), pages 1041–1056, 2015.

[5] Anna Sapienza, Alessandro Bessi, Saranya Damodaran, Paulo Shakarian, Kristina Lerman, and Emilio Ferrara. Early warnings of cyber threats in online discussions. In 2017 IEEE International Conference on Data Mining Workshops (ICDMW), pages 667–674. IEEE, 2017.

[6] Eric Nunes, Ahmad Diab, Andrew Gunn, Ericsson Marin, Vineet Mishra, Vivin Paliath, John Robertson, Jana Shakarian, Amanda Thart, and Paulo Shakarian. Darknet and deepnet mining for proactive cybersecurity threat intelligence. In 2016 IEEE Conference on Intelligence and Security Informatics (ISI), pages 7–12. IEEE, 2016.

[7] Bert-Jaap Koops, Jaap-Henk Hoepman, and Ronald Leenes. Open-source intelligence and privacy by design. Computer Law & Security Review, 29(6):676–688, 2013.

[8] Rodrigo Campiolo, Luiz Arthur F Santos, Daniel Macêdo Batista, and Marco Aurélio Gerosa. Evaluating the utilization of twitter messages as a source of security alerts. In Proceedings of the 28th Annual ACM Symposium on Applied Computing, pages 942–943, 2013.

[9] Sudip Mittal, Prajit Kumar Das, Varish Mulwad, Anupam Joshi, and Tim Finin. Cybertwitter: Using twitter to generate alerts for cybersecurity threats and vulnerabilities. In 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pages 860–867. IEEE, 2016.

[10] Bertrand De Longueville, Robin S Smith, and Gianluca Luraschi. " omg, from here, i can see the flames!" a use case of mining location based social networks to acquire spatio-temporal data on forest fires. In Proceedings of the 2009 international workshop on location based social networks, pages 73–80, 2009.

[11] Anna Sapienza, Sindhu Kiranmai Ernala, Alessandro Bessi, Kristina Lerman, and Emilio Ferrara. Discover: Mining online chatter for emerging cyber threats. In Companion Proceedings of the The Web Conference 2018, pages 983–990, 2018.