A study on proactive data-driven cyber defense through threat intelligence

アリエル, ロドリゲズ

出版情報：Kyushu University, 2020, 博士（学術）, 課程博士
バージョン：
権利関係：

（別紙様式2）

氏　　名　：ロドリゲズ　アリエル

論 文 名　：A study on proactive data-driven cyber defense through threat intelligence

（脅威収集情報によるデータに基づいた先読みサイバー防御に関する研究）

区　　分　：甲

論 文 内 容 の 要 旨

In recent years technology has implanted itself into our society and has rapidly become a crucial component. For many it has become an indispensable part of their daily routine, having a mobile phone within reach has become common while for others remotely working from home has become the norm. At the same time, the level to which society has become dependent on technology for its normal functioning has brought with it an abundance of ways to exploit those functions.

Because of these threats, it is no surprise that the importance of securing networks, devices, and systems has become a primary concern across the globe. Although a great amount of effort has been put into researching security methods, because of the speed at which new technologies are developed and implemented, it is impossible to completely secure and eliminate all vulnerabilities. Because of this, we find ourselves in a constant cycle to develop new systems to stop the next wave of threats that appear.

The purpose of this research is to investigate and develop a system that can take these aspects into account and help push research into a direction in which we can break the cycle of having to constantly be one step behind attackers. The key to achieving this and getting in front of attackers is to support the existing security infrastructure with a proactive component where potential threats are actively searched for and investigated. There is a deep need to investigate how a system can be developed and implemented which can complement the current security infrastructure to improve cyber defense in the area of pre-attack detection.

In our first contribution, we present a framework for a real-time system where we apply natural language processing techniques to Twitter data allowing us to classify and process large amounts of data to generate relevant cyber situational awareness information. This framework addresses crucial issues in this pipeline such as the filtering and integration of relevant cyber security data from a larger data stream. We consider the integration of new and emerging threat terms into our dataset to keep system filters relevant and up to date. This framework also takes advantage of the inherent context contained in textual data by leveraging sentiment analysis techniques to gain greater insights into the importance of captured threats. By tracking tweets containing security terms that have a negative sentiment we can distinguish pronounced peaks that correlate to security events which can be used by analysts. By separating these streams based on the particular security terms being used we can also gain further insight into the type of attack such as phishing, spyware, or XSS. In this way, we use information retrieval and text analysis techniques to identify, extract, and analyze emerging cybersecurity topics from the data stream.

Our second contribution builds upon the previous research by delving deeper into the data classification component of the framework. Correctly filtering out non relevant cyber security data from a larger stream of general data is a crucial piece of the system and has a huge impact on this system's output. If the data being inputted into the system is of poor quality and contains non-relevant or non-significant data points, we cannot expect a reliable output. Because of this the effective filtering and mining of data can be the most important component of this system. To address this, we present an original method called the multi-layer keyword filtering method to classify cyber security-related text

data. This method builds upon traditional keyword filtering methods by integrating a word embedding-based filtering layer which is used to limit false-positives from being retrieved from data streams. This method achieves an F1-Score of 0.99 on various subsets of our dataset and does especially well with short unstructured textual data. This can be attributed in part to the addition of our associated word list which gave up to a 7.8% increase in F1-Score. This is further expanded by introducing a clustering function on post classified data. By clustering our classified data we were able to identify non-significant data points such as advertising and marketing posts which can be removed to create a higher quality data stream. By implementing this method, the quality of data inputted into a cyber threat intelligence system is increased and hence the reliability of its output improved.

Our third contribution looks at how our solution can be implemented in a production environment across organizations that either does not have the expertise, manpower, or budget to implement traditional threat intelligence systems. Threat intelligence systems have traditionally been implemented by organizations that have enough expertise and budget to implement them. This is an issue since it has left smaller businesses and individuals open to attack. Because of this, we analyze the applicability of our system against other statistical models based on key features such as processing speed, architecture, scalability, and implementation expertise. Based on these features we have been able to outline various scenarios where we can identify the ideal implementations of our system for organizations at all levels. Based on our research the overall ideal implementation of our threat intelligence system uses an ensemble learning method including our multi-layer keyword filtering method. By using an ensemble method, we were able to achieve a F1-Score of 0.9652 with a processing time of 275ms achieving a good tradeoff between speed and classification. By doing this we ensure it is possible for all organizations to implement a cyber threat intelligence system by lowering the barrier of entry and hence increasing the level of security across all organizations.

Through the development and implementation of this research, we have found that open-source intelligence platforms such as social media, forums, and other sources are a rich source of various types of threat intelligence information. Using our method, high-quality data can be effectively mined from these sources and used within a cyber threat intelligence system to create indicators that can assist in achieving a better understanding of the cyber threat landscape. This information can subsequently be used to actively implement defense measures in a network to decrease the risk of being compromised.

This research contributes to the existing cybersecurity knowledge base by investigating, developing, and implementing a systems-based solution which assists in proactive cyber defense using cyber threat intelligence. By investigating and creating this system we have taken a step forward in finding a solution to an issue that is crucial to the current and future defense of our networks and society as a whole.