A Conceptual Scheme for Ransomware Background Knowledge Construction

Nurfadilah Ariffin
School of Computing, Universiti Teknologi Malaysia,
Johor, Malaysia
nurfadilah6@live.utm.my

Anazida Zainal
School of Computing, Universiti Teknologi Malaysia,
Johor, Malaysia
anazida@utm.my

Mohd Aizaini Maarof
School of Computing, Universiti Teknologi Malaysia,
Johor, Malaysia
aizaini@utm.my

Mohamad Nizam Kassim
Cyber Security Responsive Services Division
CyberSecurity Malaysia, 43300
Seri Kembangan, Selangor
nizam@cybersecurity.my

Abstract— **Various methods have been implemented to detect and mitigate malware. Ransomware is one of the rising malware which getting attention from world due to its impact of attack in the cyber space. Detection of potential features of Malware using traditional approach and usage of text mining is nothing new. However, identifying the Ransomware related entity from external sources and unstructured textual data like forum is new exposure towards the application of text mining in malware domain. Therefore, in this paper, a conceptual scheme is proposed to construct a Background Knowledge of Ransomware which necessary to improve the accuracy of NER when classifying the Ransomware related entity from unstructured data like online forum. From this work, the analysis related to malware also could be understood by people who have no or less expertise in Malware domain since it uses the casual text representation that are obtain from user-generated content made publicly.**

Keywords—forum, Background Knowledge, Ransomware entity

I. INTRODUCTION

Malware comprises several types of families with different attack motivations. Ransomware, seems to be one of the family that gives great impact towards business and organization. Ransomware is defined as infections to the computer systems by restricting users' access to the infected system and request specific amount of ransoms to be paid to regain the access. Ransomware is mainly categorized into two, Locker and Crypto [1]. Both have different method of attack as for Locker, it uses scareware to generate payment by locking the screen. It infects and displays a message notifying the machine has been compromised by law enforcement or any authorities and demand for ransom. Crypto involves the encryption of victims' files or data with variety of encryption methods. Then, it will notify victims about the file or data encryption and demand for ransom to be paid.

With the emergence of user-generated content such as social media, forum, blogs and online news, there is huge volume of textual data which could be used to gain insight. As in malware domain, people start to use this platform to discuss on their experience, problem and knowledge related to malware. However, textual data normally in the form of unstructured or semi-structured data which could not be used directly as knowledge representation [2][3][4].

The objective of this paper is to propose a conceptual scheme of constructing Background Knowledge in identifying Ransomware information from unstructured data such as forum. The concept proposed aims to construct the Background Knowledge of Ransomware which can be used to increase the NER accuracy in extracting Ransomware related entity from unstructured data. However, this study still in the identification phase where several Ransomware entities are manually identified and it can be used in performing the classification of Ransomware related entity.

II. RELATED WORK

A. Ransomware Background Knowledge Construction

Purpose of Background Knowledge is to gain sufficient semantic information by retrieve the term in external sources knowledge [5]. Background Knowledge has been used as the enrichment and extension of information in handling the shortage of information within particular textual data like forum, Twitter or microblog [6][7], replacing human expertise in verifying event detection system [8] and also [9] implement Background Knowledge as ontology for automated taxonomy learning of particular domain.

Background Knowledge in this study refers to the Ransomware ontology where it helps in performing behavioral analysis using unstructured textual data like forum. There are several studies that construct ontology for cyber security and malware domain. A study by [10] had proposed an ontology called digital evidence of malware which defined five classes of malware attack using clustering technique. The ontology benefits in profiling the malware attack and it can be used as forensic evidence.

Study by [11] had proposed a malware ontology based on exhibited behavior that serves as a basis for future development on reasoning and detection procedures. This study has advantage where the entities used to construct the ontology are related to malware behavior when attacking computer's user which essential in profiling the malware behavior.

978-1-5386-7541-0/18/$31.00 ©2018 IEEE

Another study by [12] had proposed a cyber security ontology that can be used to train NER in classifying entities related to cyber security domain which become the baseline in this study. From the related works by [10][11][12] in ontology construction being discussed, the concept adapted to this study where Background Knowledge is used in identifying the related entities for Ransomware classification from unstructured data like forum.

B. Extraction of Malware features

Instead of using malware sample file to perform static analysis to observe the behavior of malware , this type of analysis could also use information from unstructured text like user-generated content (forum, social media, online news) [3][4][13]. A study by [13] had extracted the features by mining the human-generated reports on malware analysis to characterize the unwanted behavior in mobile application. However, the extraction and selection of features based on the ranked keywords in which the relation and semantic of the keywords were neglected. Study by [3] had identified mobile malware within hacker forum. The extraction was performed on the attachment only that provided by the forum user where the context of the discussion was neglected.

Another study conducted by [4] differs in objective of features extraction where it used to measure the impact of malware problem among the computer users within a forum. The estimation of the malware impact depends on the frequency of malware-related terms extracted which could be enhanced by extracting semantic within the text.

III. Approach

Below is the description of terminologies used in this paper:

Background Knowledge comprises of Ransomware ontology that consists the Ransomware entities and their relationships with one another.

Property is the attributes that used in profiling the Ransomware into different family.

Features are set of keywords that are used to classify the properties belong to Ransomware.

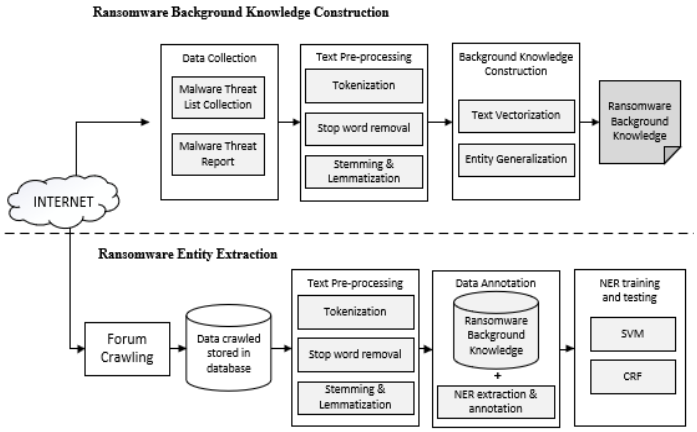

Fig. 1. Proposed Scheme

A. Sources to Construct Ransomware Background Knowledge

In this early phase, preliminary study of this research field is conducted to formulate the research problem and reviewing the literature. As stated in related works, different Background Knowledge is required for different purposes. Thus, in this proposed scheme shown in Figure 1, Background Knowledge provides an ontology for Ransomware entities classification from unstructured text. It works in providing more information regarding Ransomware which helps in overcoming the sparseness of unstructured textual data like forum. Background Knowledge could be formed from different sources of information. For this study, the sources come from various Malware Reports and several Malware threat lists that are published by well-known Antivirus companies (Kaspersky, Symantec, McAfee) as being used in [4]. These two type of sources are in different structure where Malware threat list in the form of semi-structured data and Malware threat report in the form of unstructured data. From these sources, Ransomware entities are identified to perform behavioral analysis. The concept of using Background Knowledge is adapted from [12] where it will be used as knowledge base that provides the ontology of Ransomware. In this study, Background Knowledge will be used as the information enrichment in identifying and classifying Ransomware entities and also overcoming the text sparseness within forum discussion. The hypothesis is, classification of Ransomware entities within unstructured data could be improved in terms of NER accuracy with the implementation of Background Knowledge.

B. Ransomware Background Knowledge Construction

As ontology comprises of entities for particular domain, Refer to Figure 1, Malware threat lists are analyzed to find the most common properties in describing Ransomware information. This process is necessary because different Malware threat list reported the malware incidents with different properties. At first, all properties used by different Malware threat list are listed. Next, the properties are pruned if they are uncommon to each other and irrelevant to the unstructured data like forum.

For Malware Analysis reports, it undergoes different method to extract the most significant properties to describe Ransomware. The textual data from the reports are preprocessed to remove noise and tokenized the text into sentence level. Any stop words are removed to ensure only meaningful words are left to be analyzed. Then, vectorization of text is performed using TF-IDF to get the unique words and their score from reports that reported on Ransomware incident. As the list of keyword related Ransomware extracted, the properties that describe on Ransomware are identified and updated to the list of properties from previous process using Malware threat lists.

After identification process from two sources of data which are Malware threat lists and Malware threat report, there are six entities type mange to be generalized. All of them are described as follow:

Name: The name of different Ransomware family

Aliases: Variant name of Ransomware

Type: Category of Ransomware family belongs to

Discover date: The data of Ransomware being discovered

Target: The system or any application affected or targeted by the Ransomware

Infection vector: Method or platform used by Ransomware to spread

C. Ransomware Entity Extraction

As shown in Figure 1, Ransomware entity extraction deals with entity extraction and classification of Ransomware entity from unstructured text with the use of Background Knowledge. The entities related to Ransomware within forum discussion is extracted and classified based on Background Knowledge. The entities and their relationships are important in identifying and characterizing Ransomware where the profiling of the behavior could be produced using Background Knowledge to complement the sparse information of Ransomware in forum discussion. The entities extracted in this process will be used in the next process to train the classifier to increase the accuracy of NER in classifying the Ransomware entities within the forum posts.

The extraction and annotation of data for NER training will adopt the hybrid approach that uses rule-based approach and machine-learning approach. Rule-based approach used the Background Knowledge discuss in this paper to determine and extract the relevant entities of Ransomware within unstructured text. For machine learning-based approach, we use Snorkel to annotate and train the data based on rules defined. After the annotation process, the data will be verified with human intervention to check the annotation accuracy of Ransomware entities within data. After verification, the data will be trained using two different classifiers usually combined with NER training which are Conditional Random Field (CRF) and Support Vector Machine (SVM).

D. Evaluation Metrics

The result of NER training is evaluated using main evaluation indicators, Precision, Recall and F-measure [12][14]. Those indicators are defined by true positives, false positives and false negatives. The definition is as follows:

- *True Positive(TP):* It is a collection of those class members which are correctly labelled as belong to a particular class.
- *False Positive(FP):* It is a collection of those class members which are mislabelled as belonging to a particular class.
- *False Negative(FN):* It is a collection of those items which are not labelled for any class by system but actually they belong to some class.

IV. Result

As the study is still in the early phase, the result of the whole experiment is not included. However, the potential entities and features of Ransomware have been identified within the data sources like Malware threat list and Malware threat report.

TABLE I. IDENTIFIED RANSOMWARE ENTITIES

Entities	Features
Name	Cerber.HTV, Cryptolocker, Petya
Aliases	Cerber, Cryptolock, NotPetya
Type	encrypt file, lock screen
Discover Date	2016, 2018
Target	Windows platform, medical, Mobile device
Infection vector	Spam campaigns, exploit kit,

Table I shows the entities and features of Ransomware that were manually identified and extracted to form the Background Knowledge based on [1]. The entities are selected as it comprehensive in constructing the ontology of Ransomware. Ransomware profiling could be performed by extracting and classifying Ransomware behavior from unstructured text like forum discussion with the use of Background Knowledge.

V. Conclusion And Future Work

This study aims to address the sparseness of information in forum by proposing the use of Background Knowledge that provides the knowledge base for the extraction of Ransomware related entities. The progress of this study is at the phase of data collection and entities identification. The expected result of this research should be able to provide better accuracy in NER classification of Ransomware from unstructured data with the association of Background Knowledge. The NER model produced at the end of the study could be used to determine the new Ransomware family from unstructured data. Thus, the result of this study may contribute to a better understanding of Ransomware issues and helps the related agencies to mitigate the widespread of Ransomware. From this work, the analysis related to malware also could be understood by people who have no or less expertise in Malware domain since it uses the casual text representation that are obtain from user-generated content made publicly.

ACKNOWLEDGEMENT

This research is funded by CyberSecurity Malaysia under strategic collaboration with Cyber Threat Intelligence Lab, School of Computing, Universiti Teknologi Malaysia.

REFERENCES

[1] K. Savage, P. Coogan, and H. Lau, "The Evolution of Ransomware," 2015.

[2] J. Faith, S. Thorburn, and T. H. Sinky, "Exploring healthcare experiences among online interactive weight loss forum users," *Comput. Human Behav.*, vol. 57, pp. 326–333, 2016.

[3] J. Grisham, S. Samtani, M. Patton, and H. Chen, "Identifying mobile malware and key threat actors in online hacker forums for proactive cyber threat intelligence," *2017 IEEE Int. Conf. Intell. Secur. Informatics Secur. Big Data, ISI 2017*, pp. 13–18, 2017.

[4] S. Amini and C. Kanich, "Characterizing the Impact of Malware Infections and Remediation Attempts Through Support Forum Analysis."

[5] Y. S. Chan and D. Roth, "Exploiting background knowledge for relation extraction," *Int. Conf. Comput. Linguist.*, no. August, pp. 152–160, 2010.

[6] Y. Man, "Feature extension for short text categorization using frequent term sets," *Procedia Comput. Sci.*, vol. 31, pp. 663–670, 2014.

[7] X. Zhang and B. Wu, "Short Text Classification based on feature extension using The N-Gram model," *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*. pp. 710–716, 2015.

[8] H. F. J. Gama, "Event labeling combining ensemble detectors and background knowledge," pp. 113–127, 2014.

[9] J. Hoxha, G. Jiang, and C. Weng, "Automated learning of domain taxonomies from text using background knowledge," *J. Biomed. Inform.*, vol. 63, pp. 295–306, 2016.

[10] J. Liu, R. Kammar, R. Sasaki, and T. Uehara, "Malware Behavior Ontology for Digital Evidence," pp. 585–586, 2017.

[11] R. Bonacin, O. Nabuco, V. M. Afonso, and M. Jino, "Ontology for Malware Behavior : a Core Model Proposal," 2014.

[12] H. Shang, R. Jiang, A. Li, and W. Wang, "A Framework to Construct Knowledge Base for Cyber Security," 2017.

[13] W. Chen, D. Aspinall, and A. D. Gordon, "A Text-Mining Approach to Explain Unwanted Behaviours," pp. 1–6, 2016.

[14] M. Majumder, U. Barman, R. Prasad, K. Saurabh, and S. K. Saha, "A Novel Technique for Name Identification from Homeopathy Diagnosis Discussion Forum," *Procedia Technol.*, vol. 6, pp. 379–386, 2012.