Journal of Theoretical and Applied Information Technology
15th February 2020. Vol.98. No 03

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RANSOMWARE DETECTION BASED ON HARDWARE SENSOR INFORMATION

* NUR HIDAYAH M. S, [1]FAIZAL M. A, [1]WARUSIA YASSIN, [1]KAMIL KUROBONOV
*[1]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia (UTeM), Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

E-mail: * nurhidayahmohdsaudi@gmail.com, faizalabdollah@utem.edu.my, s.m.warusia@utem.edu.my, kurbonovkamil@gmail.com.

ABSTRACT

Ransomware is a growing threat to the computer world that encrypts victim's data and asks for ransom for decryption key which causes financial loss and severe disruption in the organization. Despite the threat and an extremely growing number of cases of ransomware infection, various countermeasures have been proposed since the first appearance of ransomware but there is still not enough information on the approaches to detect it. Thus, this paper will perform ransomware detection using the behavioral method on information retrieved from computer sensors such as CPU, Main Memory and Disk Memory. The different classification method such as Naïve Bayes, J48 and KStar algorithm will be used to detect the ransomware attack and the measured value in term of accuracy.

Keywords: *Ransomware, Malware Detection, Hardware Performance, Classification, Machine Learning*

1. INTRODUCTION

Recently, the impact of ransomware become the great attention of researchers and cybersecurity experts as the new variant of this attack has the capability to bypassing antiviruses and anti-malware [1]. The ransomware known as cryptolocker is a type of malware that encrypting victim's files and request money in exchange for the key to decrypt the file [2]. Ransomware also initiates an attack immediately once installation and typically uses a countdown clock to alert the casualty. According to [3], ransomware attacks can be distinguished by using their behavior of attack and the time taken to launches the attack.

Furthermore, [4] stated that locker-ransomware and crypto-ransomware are two types of ransomware. Locker-ransomware does not encrypt or harm the victim's data on the device but block the user's access to device. This type of ransomware usually infects computers through illegal websites and forcing the victim to pay fine for accessing illegal content of the website [5]. Meanwhile, the crypto-ransomware uses a cryptoviral extortion attack, which means it encrypts data on the casualty device and demands ransom for the decryption key to unlock the data. Typically, this type of ransomware will give the message to the victims to pay the ransom within the given time [5]. Besides, crypto-ransomware has taken the advantages of modern cryptography technology to corrupt information stored and monetize the process by demanding ransom for almost three decades [6] and has caused the loss of millions of dollars on end-users and corporations.

In addition, WannaCry was one of the biggest ransomware attacks. This statement supported by [7], who said that the WannaCry ransomware requires 24 hours to contaminate 200,000 computers influencing companies such as Renault, Nissan, Telefonica Spain, FedEx. This sort of ransomware attacks to PCs legitimately, executing unchecked email connections, and malware downloaded by exploited people from site pages.

However, due to advances in cryptography and usage of different cryptosystems in ransomware structure, it is typically impossible to find the decryption key and restore the data. The best practice of not falling on attacker's demands is to always perform a backup of data, so once infected the data can be restored. Therefore, this paper will focus on the detection of ransomware by using behavioral method at a sensor-based approach. The classification method also will be used to identify the best classification algorithm in detecting the ransomware at the sensor-based approach.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The remainder of this paper is presented as follows: Section 2 discusses the related study and section 3 presents the methodology used for this paper. Section 4 presents the analysis of the results. Section 5 concludes the paper and presents future work directions.

2. RELATED WORK

Lately, only a few researchers have been conducted research on ransomware detection by analyzing the behavior. Even less papers focus on hardware-based detection in malware or ransomware detection. According to [8], there are still lack of specific ransomware detection framework in scholarly circles. Table 1 shows some of analysis for ransomware detection that has been done for several researchers.

Table 1: Analysis of Ransomware Detection Methods

Author	Purpose	Methodology	Result
Hampton et al. [9]	Recognize relevant features of ransomware	Compare the Windows Application Programming Interface (API) calls between ransomware and normal operation	8 API call exist in ransomware, 4 API 4 API found in ransomware are significant degree and 6 API more than three standard deviations.
M. Rhode et al. [10]	Collect behavioral data during file execution takes 5 min to capture which malicious payload has likely been delivered by the time it is detected.	Snapshot of behavioral data using recurrent neural network (RNN) about 5s and the sample executes from 0s to 20s.	Accuracy (96.01), time (19s), false positive (3.17), false negative (4.72)
Arabo et al. [11]	Collect information about systems behavior in order to detect ransomware.	Executed ransomware, malware and trusted software's on the windows machine.	Produce low false-positive and false-negative rate. The presence of malicious program can be detect by seen the value of CPU and memory usage.
Ozsoy et al. [12]	Malware-Aware Processors (MAP) - hardware-based online malware detector.	Used different features for classification, logistic regression (LR) and neural networks (NN).	For LR-based, it detect 90% of the malware with 6% false positive rate at its most optimal configuration. For NN-based, it detect 7% false positive rate with after-the-fact detection and still detect 94% of malware at runtime with the same false positive rate.
Ahmadian et al. [8]	2entFOX framework to detect high survivable ransomwares (HSR through Bayesian network-based analysis.	Analyzed Windows ransomwares' behavior and find appropriate features.	100% detection for HSR, 87.5% for LSR for the framework.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Chen et al. [13]	Dynamic ransomware detection system using data mining techniques.	Monitor the actual behaviors of software to generate API calls flow graphs (CFG). Then, data normalization and feature selection used to select informative features.	Simple Logistic (SL) algorithm outperform other algorithm with 98.2% accuracy and 97.6% detection rate respectively meanwhile, the false positive rate can be reduced to 1.2%.
Sharma et al. [14]	Dynamic malware analysis approach to detect well-known ransomware as early as possible in the system.	Live monitoring sets of behavioral indicators in order to extract Windows API call sequences and understand run-time behavior. Then, the ransomware is filtered out from benign software.	Most commonly targeted files are the text files, system files, executables and database files.
Almashhadani et al. [15]	Network-based Ransomware detection system	Set of valuable and informative network features were extracted, then classified into multiple types.	High detection accuracy for packet-level is 97.92% and flow-level is 97.08% respectively validating the effectiveness of the extracted features.
Manaar et al. [16]	Anomaly detection method using hardware performance counter (HPC) to detect suspicious behavior.	Artificial Neural Network (ANN) and Fast Fourier Transformation (FFT) are used to form precise and reliable solution for ransomware detection.	For FFT it takes approximately 3.443 seconds meanwhile for ANN it takes less as 4s with zero false positives to detect ransomware.
Basu et al. [17]	PREEMPT, malware detection method with zero overhead, low latency and high accuracy.	Machine learning is used to analyze embedded trace buffers (ETBs).	94% value of true positive and 2% value of false positive.
Mauro et al. [21]	Hardware Performance Counters (HPC) to precisely recognize crypto mining in real-time.	Used two different processors to distinguish the crypto mining ransomware.	Achieve a perfectly categorize crypto mining activity with samples of length as low as 5s.

Based on Table 1, the author [9] presents an examination of 14 strains of ransomware that contaminate Windows platforms. The patterns of API call and frequency examination are used to find the behavior patterns of ransomware in his research. The result shows that 18 Windows API calls happen more ransomware strains at frequencies ($p < 0.05$). Meanwhile, the author [10], examines the probability of an executable is suspicious or not based on a behavioral data snapshot. This research used feature input from 10 types of machine activity data metrics. Then, every 20 seconds a snapshot of the metrics are executed. The experiment result achieves accuracy with 96%, false-positive with 3.17% and false-negative with 4.72% at 19 seconds. Hence, it shows that when the amount of sequential data increase, the recurrent neural network will improve the value of accuracy.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Moreover, author [11] conduct research about ransomware. Behavior analysis is used in this research to distinguish benign applications, malware, and ransomware on the windows machine. His analysis used 7 ransomware, 41 benign software, and 34 malware samples. From the result it can be concluded that the value of CPU and memory usage can detect the presence of malicious programs. This author also calculates the weighted average and when the average is 0.5, it suspected the process to be ransomware. The author [12] has proposed a hardware-based online malware detector to differentiate malware from a legitimate program. The low-level feature such as architectural events, instructions, and memory addresses, and the mix of executed instruction types are used in this research to evaluate the performance detection using a different algorithm. Logistic regression and neural networks are two of the classification algorithm that implements in this research. Another analysis of the author [8] has suggested a 2entFOX framework to identify high survivable ransomware (HSR). In order to find a significant feature, the author analyzed the behavior of Windows ransomware. About 20 features were extracted in order to identify the most significant feature for HSR detection. The result shows the value of the threshold is 85 were the good option.

Furthermore, the author [13] study the dynamic ransomware detection system to distinguish known and unknown ransomware using data mining techniques such as Random Forest (RF), Support Vector Machine (SVM), Simple Logistic (SL) and Naive Bayes (NB) algorithms. This study collects API calls sequences and extracted API sequence of program behavior in order to generate the API calls flow graph. Then, the techniques of feature selection are applied to find the minimum number of informative features. The outcome revealed the simple logistic outperform other classifiers with 98.2% accuracy and 97.6% detection rate of ransomware. Besides, the author [14] develop early detection of ransomware by using a dynamic malware analysis approach. Microsoft Detours libraries and behavioral indicators are used to hook Windows API call sequences to recognize run-time behavior and differentiate the ransomware from benign software. The result shows about 261 of the total 300 ransomware gave a similar signature and produced the WinAPI call sequence highly accurately.

Other than that, author [15] presents a network traffic investigation of ransomware detection system. A set of numerous potential network feature is extracted and classified into packet-level and flow-level. The result obtained detection accuracy with 97.92% for packet-level and 97.08% for flow-level. Additionally, detection of suspicious behavior by using anomaly detection method is presented in [16]. HPC statistics are used to differentiate the presence of ransomware and normal behavior. In this work, ANN and FFT are two approaches to form a reliable and fast solution for ransomware detection. The result shows that it takes about 3.443 seconds for FFT meanwhile it takes less as 4s for ANN with zero false positives to distinguish ransomware.

Similarly, the author [17] proposes a malware detection method with zero overhead, low latency, and high accuracy. This research used four types of machine learning techniques to analyze embedded trace buffers in order to detect malware such as Mirai. The author monitors the internal chips of the input/output activity of the machine to detect the presence of rootkits, backdoors, and ransomware attacks. The result produced a 94% value true positive and 2% low false positive value. The advantage of his propose is the method not easy to hack as it used hardware-based. For author [21] suggested an effective method to detect the presence of crypto mining ransomware. HPC is used to profile the process of crypto mining in real-time and create discernible signatures. This research plan six different experiments with eleven distinct crypto mining in order to evaluate the detection rate of crypto mining activity. The outcome attains high performance which is a perfectly-recognized crypto mining activity with a short sample of 5s.

Based on the literature review above, it concludes that most of the researcher studies about detecting the ransomware attack by using a behavioral approach. Nonetheless, the method still lacks in differentiate the behaviours of ransomware and difficult to detect the presence of ransomware activity. The widespread ransomware attack becomes a serious threat and has sophisticated behavior which makes it quite challenges since it capable to do encryption in the file activity system and hide its malicious activity [18]. This statement is supported by the author [19] which recommended the detection of ransomware by using hardware sensor information, the maliciousness of the program can be detected

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

effectively. Similarly, with the author [20] who stated that the existence of a ransomware attack can be discovered by using sensors that monitor the state of internal hardware components. Therefore, this research will propose ransomware detection based on hardware sensor information.

In addition, discovering the significant parameter/attribute based on a hardware sensor is very important as it can notice the existence of a ransomware attack in the machine. Nevertheless, there is no specific research propose on the parameter/attribute in detecting ransomware activity in the machine. The existing research more focuses on technique to detect ransomware rather than mentioning the influence parameter/attribute in ransomware detection. Hence, this research will suggest the significant parameter/attribute can be used to distinguish ransomware attacks by using hardware sensor information.

3. METHODOLOGY

In this research, there are four phase implemented as shown in Figure 1.

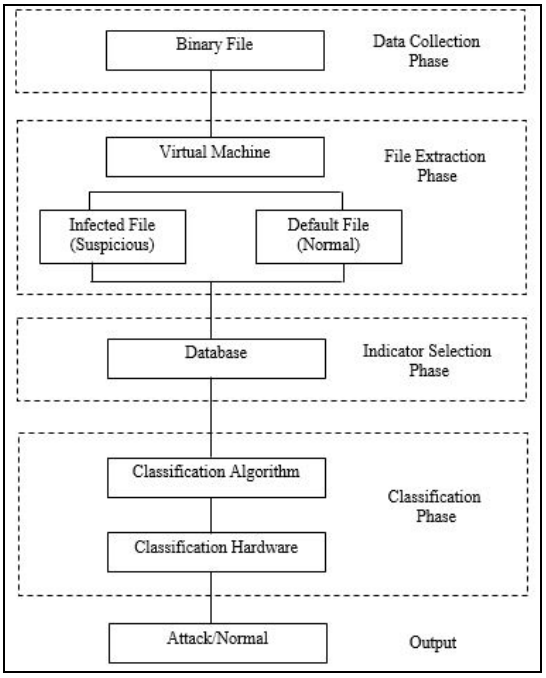

Figure 1: Ransomware Detection Model

3.1 Data Collection Phase

The data set of hardware counter collected contains a total of 174,991 records and 30 attributes. The Performance Monitor software was set to capture the performance state each second (1 record per second). Each instance in the log file will represent the state of the computer at that given time. Out of the total number of records 141,349 records are normal state reading and the remaining 33,642 are infected readings. The ratio of normal to infected data is 4 to 1. The ransomware used in this research divided into two groups consist of unclassified samples and classified samples such as TeslaCrypt, Vipasana, Cerber and WannaCry. The normal data has been captured by executed the normal sample activities in 1) idle state of the machine with no applications running, (2) Google Chrome running YouTube videos, (3) videos and music played on the device by means of K-Lite codec pack player. After starting any of these scenarios, the data collector set predefined in the virtual machine snapshot has to be started. Once the collected data is enough the data collector in Performance Monitor has to be stopped and generated log file retrieved for further analysis. Meanwhile, for ransomware data, the sample will be executed in the machine and the data collector has to be activated. Once the ransomware finishes execution, it will give the notification and description of the ransom for a user. Then, the data collector must be stopped and data generated retrieved.

3.2 File Extraction Phase

For extraction phases, all the information log will be captured after the binary file (malware and normal) is run in a virtual machine. Then, two types of data that are extracted; first, default file (normal activities) and second infected file (suspicious activities). After that, the data was labeled to 0 (normal) and 1 (infected).

3.3 Indicator Selection Phase

The captured data contain both normal and infected states will be analyzed and only significant attributes are selected. The redundant and duplicated performance counter attributes will be removed. After the elimination of the redundant attributes from the captured dataset, the data has to be converted to ARFF file format and filtered using Numeric to Nominal filter in order to be able to run the classification. The performance counter attributes in this research are:

a) Process(_Total)\% Privileged Time
b) Processor(_Total)\% C1 Time
c) Processor(_Total)\% Processor Time

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

d) Processor(_Total)\% User Time
e) Processor(_Total)\Interrupts/sec
f) Processor Information(_Total)\%Processor Utility
g) System\Processor Queue Length
h) Memory\Available Bytes
i) Memory\Pages/sec
j) LogicalDisk(C:)\Avg. Disk sec/Read
k) LogicalDisk(C:)\Avg. Disk sec/Write
l) LogicalDisk(C:)\Avg. Disk Queue Length
m) LogicalDisk(C:)\Disk Bytes/sec
n) LogicalDisk(C:)\Disk Transfers/sec
o) LogicalDisk(C:)\Current Disk Queue Length
p) PhysicalDisk(_Total)\Avg. Disk sec/Write
q) PhysicalDisk(_Total)\Avg. Disk sec/Read
r) PhysicalDisk(_Total)\Avg. Disk Queue Length
s) PhysicalDisk(_Total)\Disk Bytes/sec
t) PhysicalDisk(_Total)\Disk Transfers/sec
u) PhysicalDisk(_Total)\Current Disk Queue Length
v) PhysicalDisk(_Total)\Disk Read Bytes/sec
w) PhysicalDisk(_Total)\Disk Write Bytes/sec

3.4 Classification Phase

In this phase, the extraction data analyzed by using three selected algorithms such as Naïve Bayes, J48 and KStar to perform ransomware detection. Then, the result from the best performance of the classifier algorithm will be used to performed hardware category classification. The performance of classification detection is evaluated based on the following measurement:

a) False Positive (FP) is the amount of normal incorrectly detected as an attack.
b) True Positive (TP) is the amount of attack that has been detected accurately.
c) False Negative (FN) is the amount of attack incorrectly detected as normal.
d) True Negative (TN) is the amount of the normal that has been detected accurately.

In general, accuracy is used to study the performance of classification using selected features by using the following formula:

$$\text{Accuracy} = (TP+TN) / (TP+TN+FP+FN) \quad (1)$$

4. RESULT AND DISCUSSION

The result of this research is based on ransomware detection via three chosen classifiers algorithm. Then, the result from the best performance of the classifier algorithm will be used to performed hardware category classification. After that, the comparison between four different hardware categories is conducted to find which hardware provides the most noticeable data to be used in ransomware detection.

4.1 Classification Algorithm

This section will perform classification by using three different classifier algorithms such as Naïve Bayes, J48 and KStar in order to find the best classifier for ransomware detection.

4.1.1 Naïve bayes

The algorithm used with percentage split testing mode has tested the data in 0.44 seconds and shown 92.23% of correctly identified instances. From 59,497 instances of testing data, 55,474 were classified correctly and 4,023 instances were modeled incorrectly. As can be seen from Table 2 the results obtained from performing Naïve Bayes classification can be described as successful. Confusion matrix displays that 2,235 instances of normal data were identified wrongly, and 1,788 instances of infected data were identified as normal.

From the data presented in Table 2 and 3, it can determine the percentage of correctly identified instances. The true positive rate of the algorithm is 95.3% which shows the amount of the correctly identified normal data percentage. The classifier has identified 84.4% of the infected data correctly which is a representation of true negative results.

4.1.2 J48

The algorithm has taken 31.78 seconds to build a model and 0.08 seconds to perform the testing. Out of 20,400 testing instances, 18,850 were correctly identified and 1,550 were classified incorrectly. The percentage of correct classifications is 92.402%. Table 4 gives detailed statistics of the model's performance on testing instances. Which shows almost similar values as the Naïve Bayes algorithm.

Confusion matrix on Table 5 displays classification numbers of the performed algorithm. As can be seen, the classifier has correctly identified 9,802 unknown tuples out of 10,265 as normal, which gives the true positive rate of 95.5%.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The true negative classification rate is 9048 instances out of 10,135, which is 89.3%.

4.1.3 KStar

The classifier has taken 0.01 seconds to build a model and 57 minutes to test the model. The algorithms had taken a dataset of 60,000 records out of which 20,400 were training data. Out of 20,400 instances, KStar correctly identified 19,173 records with 93.98% detection rate. Table 6 provides detailed accuracy statistics of the KStar algorithm.

As can be seen from the confusion matrix in Table 7, the classifier has identified 10011 true positive results which give a rate of 97.5% of true positive detection. The detection rate of the infected tuples is 90.4%, the algorithm correctly identified 9,162 instances out of 10,135.

Table 2: Classification of Naive Bayes

Algorithm	Accuracy	TP Rate	FN Rate	TN Rate	FP Rate
NaïveBayes	92.23%	95.3%	4.7%	84.4%	15.6%

Table 3: Confusion Matrix of Naive Bayes

Normal	Infected	Outcome
45806	2235	Normal
1788	9668	Infected

Table 4: Classification of J48

Algorithm	Accuracy	TP Rate	FN Rate	TN Rate	FP Rate
J48	92.402%	95.5%	4.5%	89.3%	10.7%

Table 5: Confusion Matrix of J48

Normal	Infected	Outcome
9802	463	Normal
1087	9048	Infected

Table 6: Classification of KStar

Algorithm	Accuracy	TP Rate	FN Rate	TN Rate	FP Rate
KStar	93.98%	97.5%	2.5%	90.4%	9.6%

Table 7: Confusion Matrix of KStar

Normal	Infected	Outcome
10011	254	Normal
973	9162	Infected

4.1.4 Algorithm comparison

Based on the results gathered it can be said that all three algorithms are suitable for detecting the infection of the machine, due to the fact that all of the algorithms have shown a high classification rate of unknown data. Based on correctly classified data rate KStar has shown the best result of 93.98% as can be seen in Table 8. Despite the fact that the Naïve Bayes classifier has shown the worst result among three algorithms tested it was the only algorithm capable of classifying complete data set of 174,991 without any reduction as it has been done in KStar and J48.

The confusion matrix of all algorithms presented in Table 9 shows the rate of correctly and incorrectly detected numbers of instances. KStar and J48 had similar data set and KStar has made less false-positive results and false-negative results. Based on the percentage of correctly identified infected instances KStar has shown 90.4% which is the best result compared to 89.3% of J48 and 84.4% of Naïve Bayes.

.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 8: Comparison Classification Algorithm

Algorithm	Accuracy	TP Rate	FN Rate	TN Rate	FP Rate
Naïve Bayes	92.23%	95.3%	4.7%	84.4%	15.6%
J48	92.402%	95.5%	4.5%	89.3%	10.7%
KStar	93.98%	97.5%	2.5%	90.4%	9.6%

Table 9: Comparison Confusion Matrix

Algorithm	Normal	Infected	Outcome
Naïve Bayes	45806	2235	Normal
	1788	9668	Infected
J48	9802	463	Normal
	1087	9048	Infected
KStar	10011	254	Normal
	973	9162	Infected

4.2 Classification Hardware

This section will perform classification of the data set separated to hardware categories: Processor, Memory, Physical Disk and Logical Disk. This classification is going to be performed to better understand the value of each hardware category and help further researchers to focus on a specific group rather than using all of them. Based on results achieved in the previous section, KStar classifier has shown the best performance results for the given dataset. The hardware category classification will be performed only by the use of KStar algorithm.

4.2.1 Processor data

Classification of processor data has shown 60% of correct identification of testing data. Out of 20,400 records, 12,392 has been detected. The amount of incorrectly identified instances is 8,008. Time taken to perform the classification was 15 minutes.

Table 10 shows the amount of true positive and true negative results. The classifier has identified 6,569 instances out of 10,135 infected data correctly which is a true negative statistic. True positive results are 8,826 out of 10,265. As can be seen, the classifier has shown a better classification of normal data with a rate of 86% opposed to 64.8% of true negative results.

4.2.2 Memory data

The memory category dataset classified by KStar algorithm has shown 75.8% of correctly classified instances which are 15,467 records out of 20,400. The time taken to perform test classification was 5 minutes. True positive and true negative detection percentage rate can be seen in Table 12 where it can be seen that the detection rate is almost the same 74.3% to 77.4% respectively. From the confusion matrix, in Table 13 true positive identified instances are 7,623 and true negative of 7,844.

4.2.3 Physical disk data

The classification of physical disk data has shown 89.34% of correctness. The KStar algorithm has taken 16.7 minutes to perform. Out of 20,400 testing records, 18,228 were identified correctly and 2,172 records were identified as incorrect.

Based on the confusion matrix shown in Table 15 it can be observed that 10,026 records of normal data have been identified correctly with false positive of 239. True negative results are 8,202 as opposed to 1,933 false-negative results.

4.2.4 Logical disk data

KStar algorithm has correctly classified 89.25% instances from the Logical Disk dataset. The time taken to perform testing was 12 minutes. The training set contained 20,400 records out of which 18,228 were classified correctly and 2,172 were identified incorrectly.

The confusion matrix shown in Table 17 shows the correctly identified numbers of infected and normal instances. As can be seen, 10,034 instances of normal data were identified correctly and 8,174 instances of infected data were identified as infected.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 10: Classification of Processor Data

Category	Correctly Classified	TP Rate	FN Rate	TN Rate	FP Rate
Processor	60.74%	86%	14%	64.8%	35.2%

Table 11: Confusion Matrix of Processor Data

Normal	Infected	Outcome
8826	1439	Normal
6569	3566	Infected

Table 12: Classification of Memory Data

Category	Correctly Classified	TP Rate	FN Rate	TN Rate	FP Rate
Memory	75.81%	74.3%	25.7%	77.4%	22.6%

Table 13: Confusion Matrix of Memory Data

Normal	Infected	Outcome
7623	2642	Normal
2291	7844	Infected

Table 14: Classification of Physical Disk Data

Category	Correctly Classified	TP Rate	FN Rate	TN Rate	FP Rate
Physical Disk	89.35%	97.7%	2.3%	80.9%	19.1%

Table 15: Confusion Matrix of Physical Disk Data

Normal	Infected	Outcome
10026	239	Normal
1933	8202	Infected

Table 16: Classification of Logical Disk Data

Category	Correctly Classified	TP Rate	FN Rate	TN Rate	FP Rate
Logical Disk	89.25%	97.7%	2.3%	80.7%	19.3%

Table 17: Confusion Matrix of Logical Disk Data

Normal	Infected	Outcome
10034	231	Normal
1961	8174	Infected

4.2.5 Hardware comparison

Based on the result obtained from each category it can be seen that the disk memory category which includes physical and logical disk has shown the highest rate of correct classification as is mentioned in Table 18. Both physical and logical disk categories have shown almost identical results which means that the data presented there have almost the same values and performance dynamic. Thus, in further detection implementation instead of using both of the categories to use only one. Out of all the categories, the processor category has shown the worst classification result. Despite showing 86% true positive it had a poor classification of infected records with 64.8%. Thus, it can be deemed almost useless to use in detection.

As can be seen from Table 19 logical disk category has shown the best number of incorrectly identified infected records with the physical disk category being the second in that value. The memory category has shown almost a similar detection rate in true positive and true negative identified instances with values of 7623 and 7844 respectively. The worst detection rate of infected instances was shown by processor category.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 18: Comparison Classification Hardware

Category	Correctly Classified	TP Rate	FN Rate	TN Rate	FP Rate
Processor	60.74%	86%	14%	64,8%	35.2%
Memory	75.81%	74.3%	25.7%	77.4%	22.6%
Physical Disk	89.35%	97.7%	2.3%	80.9%	19.1%
Logical Disk	89.25%	97.7%	2.3%	80.7%	19.3%

Table 19: Comparison Confusion Matrix

Category	Normal	Infected	Outcome
Processor	8826	1439	Normal
	6569	3566	Infected
Memory	7623	2642	Normal
	2291	7844	Infected
Physical Disk	10026	239	Normal
	1933	8202	Infected
Logical Disk	10034	231	Normal
	1961	8174	Infected

Based on the overall result, it show that KStar classifier yielded the best outcomes in identifying Ransomware attack. This is because KStar classifier is more suitable for expecting the outcome variable since it indicates the increasing number of correct percentage for the classification of the attack compared to another classifier. Meanwhile, physical disk has capable to differentiate the ransomware attack since it has the better expectation. By monitor the state of internal physical disk components the maliciousness of the program can be detected effectively. Besides, this research also discover several indicator/attributes which can be use as parameter to detect the existence of ransomware in the machine. The selected attributes show in page 5.

5. OPEN RESEARCH ISSUE

Numerous researchers attempt to develop a new and better technique to detect malware but it is still inaccurate in distinguishing the malware activities and ineffective. Detecting ransomware activities becomes a new challenge due to advances in cryptography and usage of different cryptosystems in ransomware structure. Hence, identify the most significant indicator/attributes and classification algorithm in ransomware detection is a key factor to increase the accuracy of malware detection. Besides, the classification of the hardware counter also can be a factor to detect the presence of ransomware activity. Therefore, our proposed method, the KStar algorithm and physical disk is the best approach and more efficient to distinguish ransomware as it gives high accuracy in this research.

6. CONCLUSIONS AND FUTURE WORKS

This research emphasis on the using of classification algorithm and hardware sensor information to distinguish ransomware in the machine. The result shows that KStar algorithm is the best approach and more efficient to distinguish ransomware as it gives high accuracy in this research. Meanwhile, the analysis of hardware counter categories has shown that the physical disk hardware provides the most noticeable data to be used in ransomware detection based on the performance counters. Performance counters used have shown that the ransomware indeed creates a noticeable workload to the hardware components thus making the detection possible.

The main contribution of this research is to identify the best classifier algorithm and hardware counters of processors that can be used to detect the ransomware presence. Besides, the significant parameter also has been identified to detect the ransomware at a hardware-based approach. The limitation is the current research only focuses on the Windows 10 operating system. Moreover, this research only used several types of ransomware and the feature chosen in this study is suitable to detect only crypto variation ransomware and not suitable for detecting the blocker ransomware.

For future works, this research can be implemented on other operating systems such as

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Linux and MacOS. Different types of algorithms also can be used to perform the classification method for this project. Besides, develop a software that can perform the real-time analysis using classification and inform the user of the ransomware infection state.

7. ACKNOWLEDGEMENT

This work has been supported under Universiti Teknikal Malaysia Melaka research grant Gluar/CSM/2016/FTMK-CACT/100013 collaboration with Cybersecurity Malaysia. The authors would like to thank to Universiti Teknikal Malaysia Melaka, Cybersecurity Malaysia and all members of CMERP INSFORNET research group for their incredible supports in this project.

REFERENCES

[1] E. P. Torres P. and S. G. Yoo, "Detecting and neutralizing encrypting Ransomware attacks by using machine-learning techniques: A literature review," *International Journal of Applied Engineering Research*, Vol. 12, No. 18, 2017, pp. 7902–7911.

[2] MacRae, J. and Franqueira, V. N., "On Locky Ransomware, Al Capone and Brexit", In *International Conference on Digital Forensics and Cyber Crime,* October 2017, pp. 33-45.

[3] Chittooparambil, H.J., Shanmugam, B., Azam, S., Kannoorpatti, K., Jonkman, M. and Samy, G. N., "A Review of Ransomware Families and Detection Methods", In *International Conference of Reliable Information and Communication Technology*, June, 2018, pp. 588-597.

[4] Cabaj, K., Gregorczyk, M., and Mazurczyk, W., "Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics", *Computers and Electrical Engineering*, Vol. 66, 2017, pp. 353–368.

[5] Savage, K., Coogan, P., and Lau, H., "The Evolution of Ransomware", 2015, pp. 57.

[6] Hampton, N., "Ransomware : Emergence of The Cyber-extortion Menace", 2015, pp. 47–56.

[7] L. Pascu, "WannaCry hits Honda factory in Japan, 55 traffic cameras in Australia", June 2017. Available from https://businessinsights.bitdefender.com/wannacry-ransomware-victims [Accessed on October 22, 2019].

[8] Ahmadian, M. M. and Shahriari, H. R., "2entFOX: A framework for high survivable ransomwares detection", In *2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, 2016, pp. 79–84.

[9] Hampton, N., Baig, Z. and Zeadally, S., "Ransomware behavioural analysis on windows platforms", *Journal of Information Security and Applications*, Vol. 40, pp.44-51.

[10] M. Rhode, P. Burnap, and K. Jones, "Early-stage malware prediction using recurrent neural networks," *Computer & Security*, Vol. 77, 2018, pp. 578–594.

[11] Arabo, A., Dijoux, R., Poulain, T. and Chevalier, G., "Detecting Ransomware Using Process Behavior Analysis", 2019.

[12] Ozsoy, M., Khasawneh, K.N., Donovick, C., Gorelik, I., Abu-Ghazaleh, N. and Ponomarev, D., "Hardware-based malware detection using low-level architectural features", *IEEE Transactions on Computers*, Vol. 65, No. 11, 2016, pp. 3332-3344.

[13] Chen, Z.G., Kang, H.S., Yin, S.N. and Kim, S.R., "Automatic ransomware detection and analysis based on dynamic API calls flow graph", In *Proceedings of the International Conference on Research in Adaptive and Convergent Systems*, September, 2017, pp. 196-201.

[14] Sharma, H. and Kant, S., "Early Detection of Ransomware by Indicator Analysis and WinAPI Call Sequence Pattern", In *Information and Communication Technology for Intelligent Systems*, 2019, pp. 201-211.

[15] Almashhadani, A.O., Kaiiali, M., Sezer, S. and O'Kane, P., "A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware", *IEEE Access*, Vol.7, 2019, pp. 47053-47067.

[16] Alam, M., Bhattacharya, S., Mukhopadhyay, D. and Chattopadhyay, A., "Rapper: Ransomware prevention via performance counters", 2018, *arXiv preprint arXiv:1802.03909*.

[17] Basu, K., Elnaggar, R., Chakrabarty, K. and Karri, R., "PREEMPT: PReempting Malware by Examining Embedded Processor Traces", In *Proceedings of the 56th Annual Design Automation Conference*, 2019, pp. 166.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[18] Muhammad, S.R., Abdullah, R.S., Yassin, W., Faizal, M., "Discovering Ransomware Behavior by Host-Based Approach", *Journal of Theoretical & Applied Information Technology*, Vol. 97, No.14, 2019, pp. 3848-3858.

[19] Zhou, B., Gupta, A., Jahanshahi, R., Egele, M. and Joshi, A., "Can We Reliably Detect Malware Using Hardware Performance Counters?" 2019.

[20] Taylor, M.A., Smith, K.N. and Thornton, M.A., "Sensor-based Ransomware Detection.", *Future Technologies Conference*, 29-30 November 2017, Vancouver, Canada, pp.1-8.

[21] Conti, M., Gangwal, A., Lain, G. and Piazzetta, S.G., "Detecting Covert Cryptomining using HPC", 2019. *arXiv preprint arXiv:1909.00268*.