*International Research Journal of Innovations in Engineering and Technology (IRJIET)*

**ISSN (online): 2581-3048**

**Volume 6, Issue 3, pp 88-90, March-2022**

https://doi.org/10.47001/IRJIET/2022.603013

# The Evolution of Ransomware in Cybersecurity Space

**Dr. Alex Mathew**

Department of Cybersecurity, Bethany College, USA
Email ID: amathew@bethanywv.edu

***Abstract* - This paper discusses the evolution of ransomware in the cybersecurity space determining the threats of ransomware. The ransomware detection proposed in this method is based on machine learning algorithms. The proposed method applies sequences of the system API invocation as inputs. If an API log file is less than 10kb, it will not be executed properly and removed. As for the n-values, the best results are achieved when the *n*-value is an average of four.**

***Keywords:*** cybersecurity, ransomware, ransomware evolution, algorithm.

## I. INTRODUCTION

With the arising computer technology, cybersecurity has been a challenging issue and has risen with the advancement in internet facilities. Ransomware is one of the issues in cybersecurity which is an illegal business and leads to other threats. There are different forms of ransomware the cyber security. For instance, crypto-ransomware encrypts data of the victims' machine, while the locker ransomware is malware that locks the victims' machine, limiting the second users from using the machines [1]. This paper discusses the evolution of ransomware in the cybersecurity space determining the threats of ransomware.

## II. RANSOMWARE EVOLUTION

The ransomware evolution can be classified into two categories; before ransom as a service and after ransom as a service.

### A) Before Ransom as a Service

In 1989 a ransomware called AIDS Trozen came into existence and became popular as a PC cyborg [2]. The virus was developed by Joseph Poppa and transferred using a floppy disk. A bulk attack by the ransomware was experienced in 2011 by internet users. The first quarter saw over 30000 types of ransomware, while the third quarter saw over 60000 ransomwares. The ransomware attack later grew in 2015 with the new type of crypto locker introduced. During this period, ransomware was started with TOR as a service that provided ransomware services at about 20% commission.

### B) After Ransom as a Service

The frequency of ransomware attacks increased with the ransomware on commission. Some ransomware includes Locker Pin, which infected the android systems by changing the PIN, iteration of Crypto wall, which helped the criminals avoid detection and Petya, which makes it hard to access the hard disk until the payment of ransom is done [3]. The evolution of ransomware is continuing with the advancement of technological devices and the congestion on the internet by many users, either at the individual level or at the company level.

## III. RANSOMWARE INFECTION

A user has four options once infected by the ransomware: paying the ransom, restoring from the backup, losing the files, and brute-forcing the key. The ransomware criminals target large companies and affluent countries for their data. The initial attacks were on the windows platforms, but currently, the ransomware infects even the android systems and apple while others infect smartwatches in the form of IoT devices. The scalable vector graphics is the current mode of attack by ransomware.

## IV. PROPOSED METHODOLOGY

A ransomware detection proposed in this method is based on machine learning algorithms. The flow chart shown in figure 1 below shows the processes of the proposed method adopted.

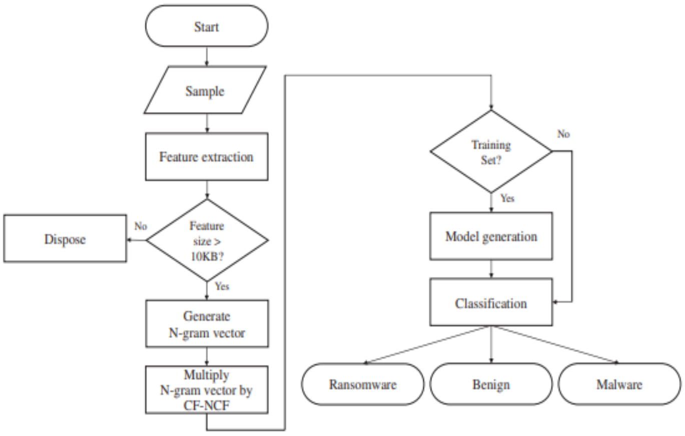


**Figure 1: The flowchart of the proposed method**

Each extracted API sequence is processed for each sample, and generation of the *n*-gram sequences occurs [4]. Input vectors are then generated from the *n*-gram sequences. The input vector elements are represented as one if each *n*-gram appears of the sequences of the *n*-gram, and the 0 will be represented if the *n*-gram doesn't appear. To determine the weights of each element, the calculation of the Class frequency Non-Class frequency of the elements of the generated vectors will be carried out. The generated vectors with the weights will generate a classification model. Six machine learning algorithms are used to describe the detection model for classifying the unknown binary samples into benign files, ransomware or malware.

### A) Experiments

The proposed method applies sequences of the system API invocation as inputs. The extraction of the sequences of Windows native API invocation is done using the dynamic binary instrumentation (DBI) of the intel PIN tool, as shown in figure 3 below. The virtual execution environment is set up using windows 7 with 32-bit OS 16GB RAM of the guest machines while the host machine is the Ubuntu 16.04 64-bit OS [5].

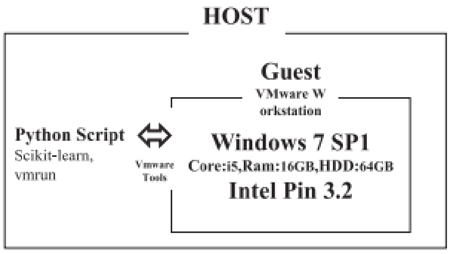


**Figure 2: The setting of the experiment environment**

Python scripts execute the executable input files, and the guest machine stores the execution results. The vmrun utility does the automated execution. The commands of the vmrun are sent to the guest machine on the environments of the virtual machine. The automatic execution process is as follows.

i. Saving of the snapshot on the guest machine is done on the machine's clean state.
ii. A process is created to receive the vmrun file of the guest machine, and the commands of the vmrun are then transferred to the host machine.
iii. The process created undertakes the sampling of the executable file, which leads to the extraction of the Windows Native API invocation log. The execution is done in a controlled environment to achieve one of the following conditions [6].
    - API invocations are greater than 50000
    - The execution time exceeds five minutes
    - The execution of the file is terminated

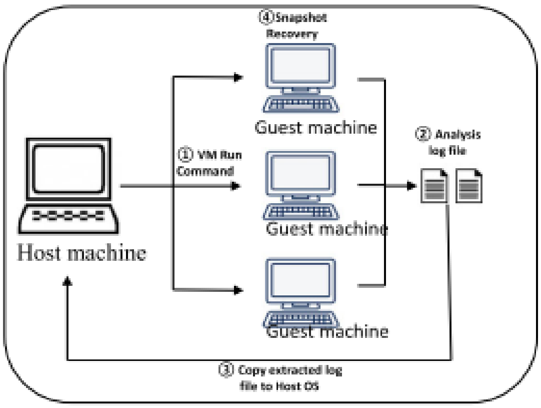
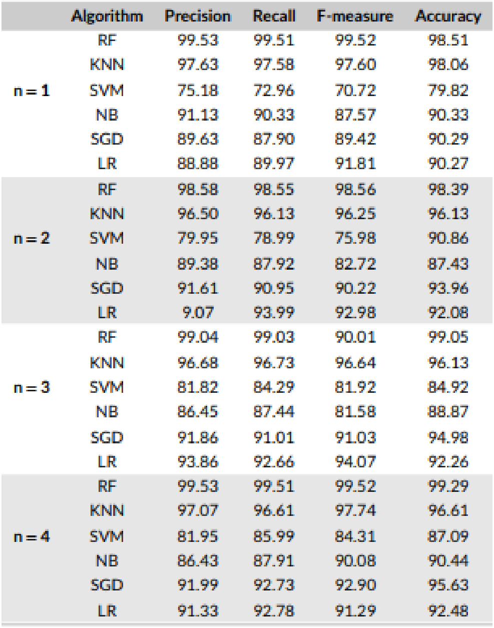


**Figure 3: Automated execution**

The algorithms chosen in this process include the random forest (RF), Logistic Regression (LR), Naïve Bayes (NB), Stochastic Gradient Descent (SGD), K-Nearest Neighbors (KNN) and Support Vector Machine (SVM).

## V. RESULTS ANALYSIS

If an API log file is less than 10kb, it will not be executed properly and removed. As for the n-values, the best results are achieved when the n-value is an average of four. With the increased n-value, the APIs are in one unit [7]. If n is as small as 1, the malicious behavior will not be fully focused. The n-value needs to be set to a more reasonable value that can detect malicious behavior. The detection accuracy in this method is about 97% which shows that this method can lead to the separation of ransomware from other malware. The results for different algorithms are shown in figure 4 below.



| | Algorithm | Precision | Recall | F-measure | Accuracy |
|---|---|---|---|---|---|
| n = 1 | RF | 99.53 | 99.51 | 99.52 | 98.51 |
| | KNN | 97.63 | 97.58 | 97.60 | 98.06 |
| | SVM | 75.18 | 72.96 | 70.72 | 79.82 |
| | NB | 91.13 | 90.33 | 87.57 | 90.33 |
| | SGD | 89.63 | 87.90 | 89.42 | 90.29 |
| | LR | 88.88 | 89.97 | 91.81 | 90.27 |
| n = 2 | RF | 98.58 | 98.55 | 98.56 | 98.39 |
| | KNN | 96.50 | 96.13 | 96.25 | 96.13 |
| | SVM | 79.95 | 78.99 | 75.98 | 90.86 |
| | NB | 89.38 | 87.92 | 82.72 | 87.43 |
| | SGD | 91.61 | 90.95 | 90.22 | 93.96 |
| | LR | 9.07 | 93.99 | 92.98 | 92.08 |
| n = 3 | RF | 99.04 | 99.03 | 90.01 | 99.05 |
| | KNN | 96.68 | 96.73 | 96.64 | 96.13 |
| | SVM | 81.82 | 84.29 | 81.92 | 84.92 |
| | NB | 86.45 | 87.44 | 81.58 | 88.87 |
| | SGD | 91.86 | 91.01 | 91.03 | 94.98 |
| | LR | 93.86 | 92.66 | 94.07 | 92.26 |
| n = 4 | RF | 99.53 | 99.51 | 99.52 | 99.29 |
| | KNN | 97.07 | 96.61 | 97.74 | 96.61 |
| | SVM | 81.95 | 85.99 | 84.31 | 87.09 |
| | NB | 86.43 | 87.91 | 90.08 | 90.44 |
| | SGD | 91.99 | 92.73 | 92.90 | 95.63 |
| | LR | 91.33 | 92.78 | 91.29 | 92.48 |

**Figure 4: Table of results when *n*=1, 2, 3 and 4**

## VI. CONCLUSION

With the arising computer technology, cybersecurity has been a challenging issue and has risen with the advancement in internet facilities. This paper discussed the evolution of ransomware in the cybersecurity space determining the threats of ransomware. The ransomware evolution can be classified into two categories; before ransom as a service and after ransom as a service. The ransomware detection proposed in this method is based on machine learning algorithms.

## REFERENCES

[1] D. Zhuravchak, "RANSOMWARE SPREAD PREVENTION SYSTEM USING PYTHON, AUDITD AND LINUX", *Cybersecurity: Education, Science, Technique*, vol. 4, no. 12, pp. 108-116, 2021. Available:10.28925/2663-4023.2021.12.108116.

[2] S.Fuloria, "Cybersecurity and Ransomware," *Academia Letters*, 2022. Available: 10.20935/al4820.

[3] Y. ITAI and E. Onwubiko, "Impact of Ransomware on Cybersecurity," *INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY*, vol. 17, no. 1, pp. 7077-7080, 2018. Available: 10.24297/ijct.v17i1.6750.

[4] M. Byrne, "Cybersecurity and the New Age of Ransomware Attacks," *Journal of Peri Anesthesia Nursing*, vol. 36, no. 5, pp. 594-596, 2021. Available: 10.1016/j.jopan.2021.07.004.

[5] A.Mohammad, "Ransomware Evolution, Growth and Recommendation for Detection," *Modern Applied Science*, vol. 14, no. 3, p. 68, 2020. Available: 10.5539/mas.v14n3p68.

[6] S. Yadav, "A Survey on Ransomware Malware and Ransomware Detection Techniques," *International Journal for Research in Applied Science and Engineering Technology*, vol. 10, no. 1, pp. 243-248, 2022. Available: 10.22214/ijraset.2022.39787.

[7] S. Alsoghyer and I. Almomani, "Ransomware Detection System for Android Applications," *Electronics*, vol. 8, no. 8, p. 868, 2019. Available: 10.3390/electronics8080868.

**Citation of this Article:**

Dr. Alex Mathew, "The Evolution of Ransomware in Cybersecurity Space" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 6, Issue 3, pp 88-90, March 2022. Article DOI https://doi.org/10.47001/IRJIET/2022.603013

*******