International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 11, No.1 (Mar-2022)

https://dx.doi.org/10.12785/ijcds/110195

Critical Feature Selection for Machine Learning Approaches to Detect Ransomware

Sachin Malik[1], Bharanidharan Shanmugam[2], Krishnan Kannorpatti[2] and Sami Azam[1]

[1]*College of Engineering, IT and Environment, Charles Darwin University, Darwin, Australia*
[2]*Energy and Resources Institute, College of Engineering, IT and Environment, Charles Darwin University, Darwin, Australia*

Received 28 Jul. 2021, Revised 20 Feb. 2022, Accepted 9 Mar. 2022, Published 31 Mar. 2022

Abstract: It has been nearly three decades since the first strain of ransomware surfaced online, but still, it is one of the most destructive malwares of all time, costing millions of dollars around the globe each year. Ransomware is a type of malware that encrypts all the data on an infected device using asymmetric encryption algorithms and demands a ransom to decrypt the data. As it is nearly impossible to recover the encrypted data without having a backup, victims end up paying the ransom or lose the data. Therefore, the best approach is to detect the ransomware at its initial stages and remove it before any damage is done. Traditional methods of signature-based detection are useless against the newer ransomware families as they exhibit polymorphic techniques and change their signatures frequently. This paper critically reviews some of the existing detection methods that use behavioural analysis using machine learning techniques. To test the efficiency and accuracy of various machine learning algorithms, logs from an infected windows machine were analysed using supervised machine learning algorithms to classify it as ransomware or non-ransomware. Secondly, the datasets were split into training and testing set to check the accuracy of the trained models and finally the most important behavioural features were determined that are most crucial in differentiating a log file from a ransomware infected machine to that of an uninfected machine.

Keywords: Ransomware, Encryption, Malware, Polymorphic Techniques, Behavioural Analysis

1. Introduction and Overview

Ransomware is a class of malware that targets the availability of user data files by encrypting the data using complex encryption algorithms or by locking the victim's computer, to prevent the user from accessing it [1]. It uses people's fear of losing their personal or sensitive information stored on the computer to extort money in form of ransom to unlock the victim's computer or decrypt the encrypted files [2]. The preferred payment methods used by criminals is through cryptocurrency (most preferred: Bitcoins), due to their untraceable nature of transactions. Ransomware can be broadly classified into two categories: the first is locker-ransomware, it is designed to lock the victim's computer, thus rendering it unusable; the second is crypto-ransomware, it is designed to encrypt the files located on the victim's computer to make them inutile [3]. In both cases, the victim is then asked to pay some ransom to get access to their data.

The first ransomware named "AIDS Trojan" is dated back to 1989 [4]. While ransomware has been a threat for almost three decades, but recently it has become more prominent due to an enormous number of ransomware variants and victims. It was near to impossible to monetize such attacks in the pre-web age but now with a plethora of anonymous online payment services, there is plenty of scope for cybercriminals to launch such types of attacks.

Most of the anti-virus companies are struggling to keep up with the pace of evolving malware variants. As anti-virus uses signature-based mechanisms to detect malware, criminals implement very sophisticated packing techniques to elude detection. Moreover, online services, such as ransomware-as-a-service (RaaS), have made it very easy for cyber-criminals to construct their version of ransomware; thus, rendering the signature-based mechanisms futile [5].

According to Coveware, the Average ransom payment has increased by 33% from Q4 2019 to Q1 2020. As shown in Figure 1, on average each business is paying approximately USD111,605 to get their data back in a ransomware attack [6]. Ransomware has been evolving ever since they first surfaced in 1989. Unlike the old days, computers these days have multi-core CPUs with Hyper-Threading or Simultaneous Multithreading technologies. These new technologies are used by organizations and provide huge benefits in day-to-day operations but on the other hand, modern ransomware also uses this technology of parallel computing to make the attacks faster and more harmful than ever.

E-mail address: Bharanidharan.shanmugam@cdu.edu.au

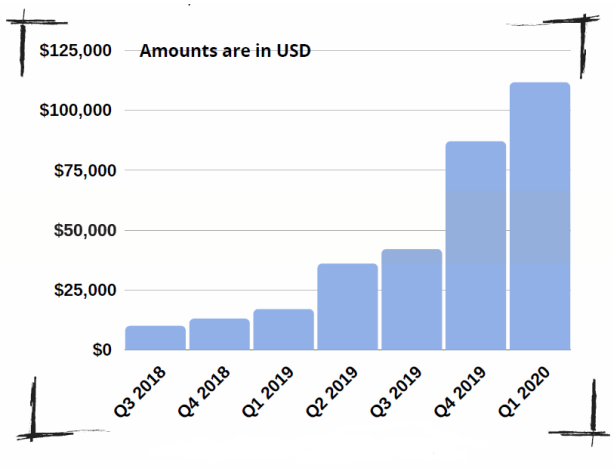

Figure 1. Average ransom paid by businesses by quarter

Old detection methods have now become useless against new types of ransomware and thus it is the need of the hour to either improve the existing detection methods or create some new methods that can be effective against new ransomware families. The main aim of this paper is to determine the most critical features that contribute to the detection of ransomware.

Rest of the paper is organized as follows: Section 2, provides a literature review of the existing research in this field of study that consists of brief history of ransomware, how ransomware attacks work and what detection methods are used to successfully detect a ransomware attack. Section 3 demonstrates the methodology of the experiments conducted in this research followed by the implementation in Section 4. Finally, results are discussion in Section 5 and Conclusion and Future work is discussed in Section 6.

A. *History of Ransomware*

Ransomware is one of the most prolific cyber threat facing the world today. It has been around for three decades [7] and it's unlikely to stop any time soon. The first trace of what we know now as ransomware was called AIDS Trojan (also known as PS Cyborg), it used symmetric-key encryption to lock the victim's device and demanded payment [4]. Symmetric-key encryption uses the same key for encryption as well as decryption, thus deploying the encryption/decryption key with the ransomware. Due to its inherent weakness, it was possible to decrypt the files and recover the data easily as compared to modern ransomware.

With the advent of the 21st century, ransomware was a frequent occurrence. In the early 2000s, ransomware became popular as Scareware [8]. People surfing the web often received a warning that some error has occurred, thus forcing users to download certain software to fix the issue. Criminals were using the symmetric-key encryption technique till 2005 but in 2006 they adopted a sturdier encryption technique called Asymmetric encryption. Asymmetric encryption uses two encryption keys known as the public key and private key. The public key is used to encrypt the data and cannot be used to decrypt data whereas the sole purpose of the private key is to decrypt the data. This concept was used by the criminals to encrypt the victim's data and keep the private key hidden until the ransom was paid [9].

Between 2011 and 2015 there was a major surge in ransomware attacks. Some major ransomware families like CryptoWall and Chimera were distributed over the internet and began attacking companies around the world [10]. The former had many versions throughout 2014 and 2015 and every new version was more sophisticated than the previous. One of the ransomware which also was in the headlines at that time was Cryptolocker ransomware. According to BBC News, cryptolocker ransomware infected about 250,000 PC's within a very short period of time [11]. According to the report, cryptolocker was using a strong third-party certified cryptography offered by Microsoft's CryptoAPI, such sophistication of this ransomware made them successful. Figure 2 shows the history timeline of some of the most infamous ransomware.

After 2015, there were other major ransomware such as WannaCry, Petya, Locky, etc., which cost billions of dollars globally. These were even more sophisticated ransomware using advanced encryption techniques and better at being anonymous. Most of the modern ransomware demand ransom in form of Bitcoins due to their untraceable nature while some use e-gift cards or iTunes gift card to accept the ransom. Moreover, since 2015 there has been an upsurge in ransomware-as-a-Service, where criminals sell variants of ransomware on the Darknet to anyone who is willing to pay them [5].

Coming to the present day, this an era of ransomware that focuses more on extortion. Today the encryption is so strong that it is virtually impossible to break. Nowadays, criminals have moved from simply infecting devices and demanding money to threatening the victim to publish data. Snake, Maze, and Sodinokibi are new variants that are discussed almost every day in the news. Evolving technology, advanced encryption techniques, obfuscated API calls, and criminals distributing variants of ransomware have rendered previously used detection techniques like static analysis and signature-based detection futile [3]. To compete with the evolving ransomware families and mitigate their effects researchers have come up with various techniques like Unveil, Shannon Entropy, Key Backup, etc., which dynamically analyse the ransomware based on its behaviour. Ransomware has evolved in so many different aspects that it is very difficult to compare and identify it from Dr. Popp's first known variant. By looking at the history of ransomware we can conclude that it is not going to stop, therefore it's better to prepare ourselves to detect ransomware before it can do any damage to our privacy, sensitive data, or business, and stop it at the very beginning.

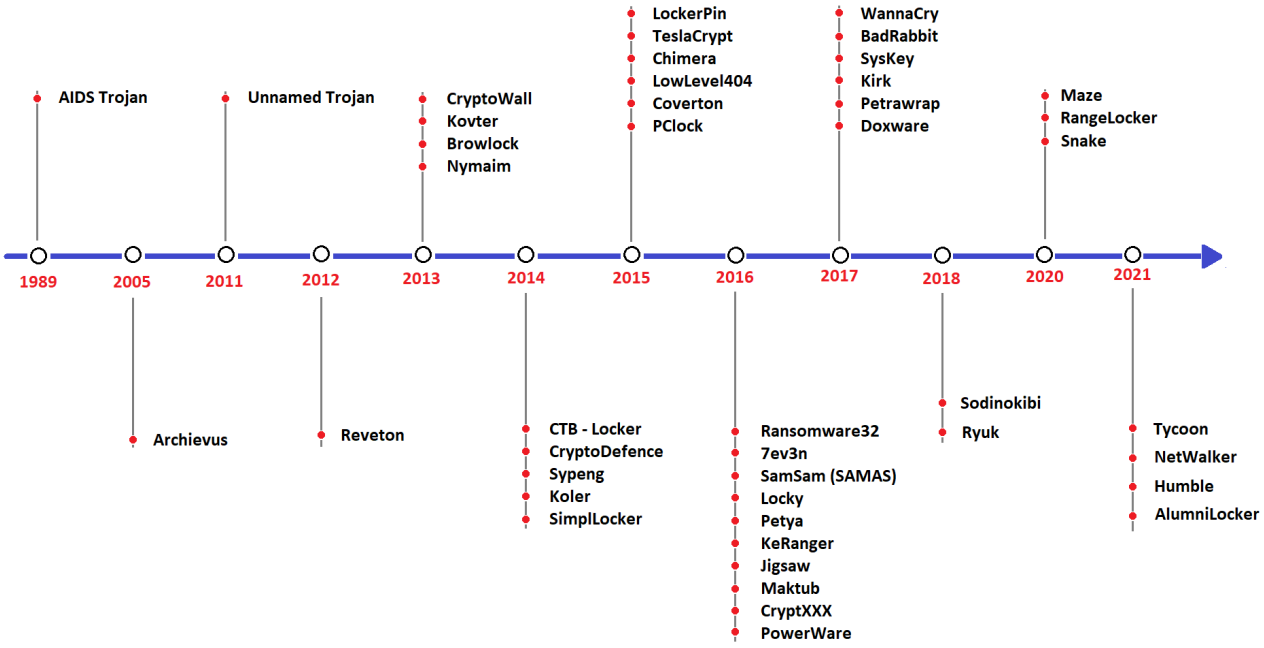

Figure 2. History timeline of some infamous ransomware

B. *Classification of ransomware families*

Ransomware can be broadly classified into two categories: Crypto ransomware and Locker ransomware [10]. Some papers suggest a third type of ransomware i.e. Hybrid ransomware [12].

1) *Crypto Ransomware*

Crypto ransomware works by scrambling sensitive data with virtually- unbreakable encryption algorithms [8]. The encryption works on the public key and private key relation, while the public key is used to encrypt the data, the private key can be used to decrypt the data but is kept hidden by the attacker until a ransom is paid. WannaCry, Locky, and CryptoLocker are some of the major ransomware of this category.

2) *Locker Ransomware*

Locker ransomware is designed in such a way that it restricts the user access to the system functions by locking the system completely [2]. Once the victim's device is infected, locker ransomware changes the access registry to block the victim from logging into the device. Moreover, it changes the bootup screen to a ransom note that instructs the victim to pay the ransom in order to unlock the system. AIDS Trojan, Petya, NotPetya, and LockerPin are some of the famous ransomware of this category.

3) *Hybrid Ransomware*

Hybrid ransomware has the characteristics of crypto ransomware as well as locker ransomware. It can lock the device of the victim along with encrypting the data stored on the device [12]. VirLock is one of the most famous hybrid ransomware that has made it to the headlines lately.

C. *Stages of ransomware attacks*

According to Silva et al. ransomware attacks can be categorised into four stages i.e. Infection, Encryption, Demand, and Outcome [13]. Figure 3 briefly describes four stages of ransomware attacks. The first stage is Infection, in this stage victim either falls prey to a phishing email and downloads the ransomware onto one's device or a malicious website is used by the adversary to install the ransomware on the victim's device. Once the ransomware is installed onto a victim's device then in the second stage of the attack the ransomware starts encrypting the files saved on the devices. Files and documents are encrypted using complex encryption algorithms to make it impossible to decrypt without the private key. In the third stage of attack i.e. Demand, usually, a ransom note pops up on the screen of the victim and demands money in Bitcoins, Dark coins, or via MoneyPak to remain untraceable. Depending on whether the victim pays the ransom or not the files and documents are either decrypted or deleted. The next sub-sections describe in detail about the four stages of ransomware attacks.

1) *Infection*

This is the first phase in any type of malware attack. In the case of ransomware attacks, during this phase attackers trick the victim into downloading malicious software using

social engineering methods such as spam mails, phishing, or spear-phishing, etc. Once the malicious software is downloaded it gets installed on the device of victim like any other normal software without alerting the victim or any other defense systems in the victim's device. After the installation is complete it either may wait for a few weeks before starting the attack or may start the attack straight away. Depending upon the type of ransomware it can try to reach all the devices on the network before starting the attack to do the maximum damage, one such example is the case of WannaCry using EternalBlue vulnerability to infect all the devices on the network [14].

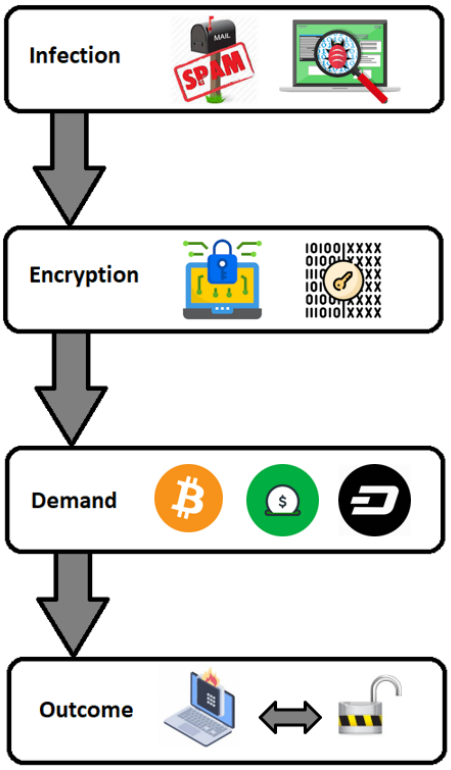

Figure 3. Four Stages of Ransomware Attacks [13]

2) Encryption

Encryption is a technique using which a plain text can be transformed into a scrambled text, also called as ciphertext. Plain text here means the general information which can be read and understood by anyone whereas the ciphertext cannot be understood by anyone until and unless a decryption key is used to convert it back to plain text [15].

3) Demand

After the data on the victim's device is encrypted the ransomware displays a ransom note explaining the attack and how the victim can pay the ransom and get their data back. Some ransomware like Maze, Sage, and GrandCrab v3 change the wallpaper of the desktop to display the ransom note and make it more intimidating whereas others such as WannaCry and Jigsaw ransomware displays a pop-up dialogue box with a timer to pressurise the victim and instructions to pay the ransom. While changing the desktop wallpaper and pop-up messages are common ways of displaying a ransom note, a new method of creating a text file on the desktop has been seen in the newer variants of ransomware families like Ryuk, Locky and Snake, the text file not only instructs the victim to pay the ransom but also threatens to delete the data or make it public after a certain time if the ransom is not paid.

4) Outcome

Depending upon what happens with the data we can categorise the outcomes into the following categories:

a) Data is recovered

If the victim chooses to pay the ransom, there is a high possibility that the data will be decrypted by the attackers. This is so because attackers want to gain the trust of the victims which will help them in getting payments from a greater number of attacks.

If the ransomware does not change the names of the document and does not overwrite the deleted data, there is a chance to recover some data using digital forensic tools.

It is possible that the victim has a full backup of the systems, therefore data can be easily recovered from the back after resetting the device.

b) Data is lost

If the victim chooses not to pay the ransom, it is certain that the data will be lost in a few days. Some ransomware deletes all of the data at once whereas some file every 3-4 hours to force the victim into paying the ransom.

Even if the data is not deleted by the ransomware it is not possible to decrypt the data therefore it will be lost in any case.

c) Data is made public

New ransomware families such as Maze, snake, Sodinokibi, etc. have been seen to make the data public if the ransom is not paid by the company. This new trend of making the data public is even more dangerous as the data can be used by other hackers to harm individuals.

Earlier strains of ransomware families were just limited to targeting the availability of the victim's data, but newer strains are targeting the confidentiality of their victims as well.

D. Detection Methods

As it is nearly impossible to recover the data once the ransomware has completed the encryption of the files, the only approach to stop ransomware is to detect it at its earliest stage and remove it before any damage is done. In recent years the research on the detection of ransomware based on its behaviour has been at its peak because of the impact and number of ransomware attack cases growing exponentially. This section consists of the review of existing

detection methods that have been proposed by various researchers around the world.

Ransomware detection can be categorised based on the input information that has been used by the detection method. Berrueta et al., categorises the detection methods into three categories based on the input data used by the detection method as Local Static, Local Dynamic and Network-Based [16].

It is possible that some detection methods use a combination of two or more types of input information[17]. To narrow the scope of this paper and achieve the previously stated goals, only those detection methods that either use local dynamic information or local dynamic information in conjunction with some other information input as parameters to machine learning algorithms will be reviewed in the further section of this chapter.

2. Literature Review

Machine learning based detection methods require more complex combination like the one suggest by Gupta et al. in their paper "AI assisted Malware Analysis: A Course for Next Generation Cybersecurity Workforce"[18].and larger number of input parameters. Most of the existing machine learning based ransomware detection methods use supervised learning; however, the unsupervised learning technique can also be seen in some of the detection methods. In the paper "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection", Sgandurra et al. has presented a machine learning approach for dynamically analysing and classifying ransomware families and named as EldeRan. Based on the application of supervised regularised logistic regression algorithm this detection method surveils a set of actions to determine whether an application is a ransomware or not. The features that are analysed by EldeRan includes windows API calls, registry key operations, file system operations, file operations on file extensions, directory operations, dropped files and the strings embedded in the binary [3].

Like EldeRan, Hwang et al. has used features like API call pattern, registry keys, file extensions etc. in their proposed two-stage ransomware mixed ransomware detection model. They have used a Markov model to categorise an application as malign or benign and a Random Forest machine learning model to control false positive and false negative errors [19]. Whereas Kharraz et al. claims that MFT (Master File Table) can be used to detect ransomware by monitoring the encryption and deletion activity of file [2]. A weakness with this argument is that much other benign software can exhibit similar file activities thus resulting in false positives; however, MFT can be used in conjunction with other parameters to provide better and accurate results.

Kirda et al. presents a novel dynamic analysis system called Unveil [20]. It is a bit unique approach in detecting the ransomware as it generates an artificial environment that is used to detect the ransomware attacks. Along with monitoring file system activity, unveil also measures the structural similarity of the screenshots from the infected device screen (samples) to the possibly infected device screen to detect the presence of ransomware this is so because most of the ransomware families display the ransom note on the desktop screen; however, the trend of displaying "ransom notes on desktop screen" is now shifting towards the "ransom notes in the text files" in newer strains of ransomware families, which will render this parameter useless.

Mehnaz et al. took a different approach to use canary files and monitoring the file encryption by increase in file entropy [21]. Along with file entropy they have classified applications based on the access primitives; for example, if a file was rapidly opened, read, and written. They tested algorithms like Naïve Bayes, Decision tree, Logistic Regression, and Random Forest, but finally chose random forest algorithm as their classifier because it proved to be faster and more scalable as compared to others. Compared to Mehnaz et al., Lee et al. have used an entropy technique to measure the characteristics of the file and applied a machine learning technique to measure the entropy of files for a backup system [22]. They have used three methods of entropy calculation to provide input to the machine learning algorithm and thus compared the results from different algorithms like Kernel Support Vector Machines, Decision Trees, k-Nearest Neighbours, and the Multi-Layer Perceptron.

Another approach for detection of ransomware is given by Abukar et al. in their paper "Automated Analysis Approach for the Detection of High Survivable ransomware" [23]. They used Term Frequency-Inverse document frequency (TF-IDF) to select features from the analysed samples of ransomware. They analysed seven features including registry paths, windows API calls, file operation, strings, directories, drops and libraries from which registry keys and API stats scored the highest when counted by TF-IDF algorithm. Further, they used Support Vector Machine (SVM) and Artificial Neural Network (ANN) to implement a machine-learning based model for detection of ransomware attacks.

3. Methodology

A. *Data Collection*

The research papers were downloaded from Academic databases like Science Direct, IEEE, CDU Library. Ransomware strains were downloaded from various open-source repositories. More details can be found in next chapter.

B. *Required Resources*

Following resources are required to conduct this research:

1) Laptop/Computer: A computer or laptop with basic specifications (Memory:16Gb, Storage: 500Gb, Processor: i7 and above, multicore etc.). Used to conduct the research, setup virtual environment and train models using machine learning algorithm.
2) Software used: Microsoft office suite, Microsoft Project, EndNote, Virtual box, Tools for analysis. Tools specific to experiments have been discussed in the next chapter.
3) Academic Database: Access to the academic database: Access to academic databases such as IEEE, Science direct, CDU Library (or any university library) to search the latest peer-reviewed research papers.
4) Access to Malware: Access to different families of ransomware and their variants.

C. Proposed Method

In any type of ransomware attack, the malware needs to inform victim that the attack took place and how the victim needs to pay the ransom. Along with the ransom notes, all ransomware families exhibit certain behaviours that are necessary for the attack to be successful; for example, accessing user files, mass encryption, modal dialogues, entropy change etc.

First, a real like virtual environment was set up using virtual box along with a DNS server where all the traffic from the victim machine will be directed to trick the ransomware into believing that it is connected to the internet, as modern ransomware strains look for virtual footprints to detect a virtual environment and tries to connect to the command-and-control server before running on the victim's machine. Therefore, setting up a real like environment with files and folders will trick the ransomware to believe that it is a victim's machine and when the ransomware tries to connect to the C&C server it will get response from our fake internet. Once the environment is set up, a ransomware strain will be injected in the environment and allowed to do its work.

Then the logs will be taken out from the infected machine and used to train machine learning models. A high-level implementation model for the detection method can be seen in Figure 4.

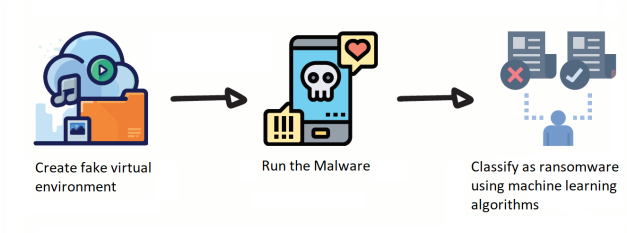

Figure 4. Approach to implement detection method

4. Implementation

A. Lab Setup and running the ransomware

For setting up the ransomware analysis environment, one of the most popular hypervisors called Virtual Box is used on a Windows 10 machine. Total of three virtual machines are setup as a part of ransomware analysis environment. Figure 5 shows the lab set up was hosted on windows 10 machine that was used to perform the experiments.

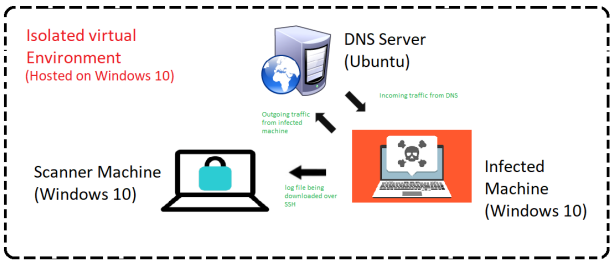

Figure 5. Lab setup for experiments

1) Windows Machine (Victim)

This is the victim machine which will be infected using various ransomware strains. Following configurations are done within this virtual machine.

a) A windows 10 virtual machine is setup with dummy data to make the environment look legit.
b) Firewall and Windows Defender is turned off intentionally to ease the execution of ransomware.
c) Following tools are installed for taking logs and monitor the machine:
Process Hacker: It is a tool that lists all the processes that are running on a machine.
Process Monitor: This tool records live file system activity such as process creation and registry changes in csv file.
Disk Pulse: This tool logs the changes in files and folders of a given directory. MS Network Monitor: It is a network monitoring tool that logs the packets sent and received on a network.
API Monitor: It monitors API calls made by any software.
d) To isolate the machine from external environment internal network is used. All the internet traffic is routed to a Linux machine hosted on the same network.

2) Linux Machine

Ubuntu is used to host internet simulator iNetsim to trick the ransomware into believing that it is connected to internet this is done by changing the default gateway and DNS server for victim machine to the address where iNetsim is hosted.

3) Windows Machine (Scanner)

This machine is hosted as an additional layer that can be used to sanitize the logs that will be taken out from the infected machine. An anti-virus has been installed to check the log file for any malicious content.

4) Downloading the ransomware samples

The binary for ransomware samples were downloaded from two following websites:

a) https://github.com/ytisf/theZoo

b) https://dasmalwerk.eu/

All the samples are in zip files protected with password ”infected”. Note: Ransomware Samples were downloaded on the victim machine before setting up the Fake network.

5) Running the ransomware

After all the configurations were done, two Crypto Locker ransomware strains known by the name of Locky and TeslaCrypt were run from the samples. Within few minutes all the files were encrypted and the file extensions were changed to “.ykcol” in case of Locky ransomware variant and “.ecc” in case of TeslaCrypt ransomware. The desktop wallpaper changed to an image on screen and a pop-up was displayed with the instructions to pay using bit coins as shown in figure 6.

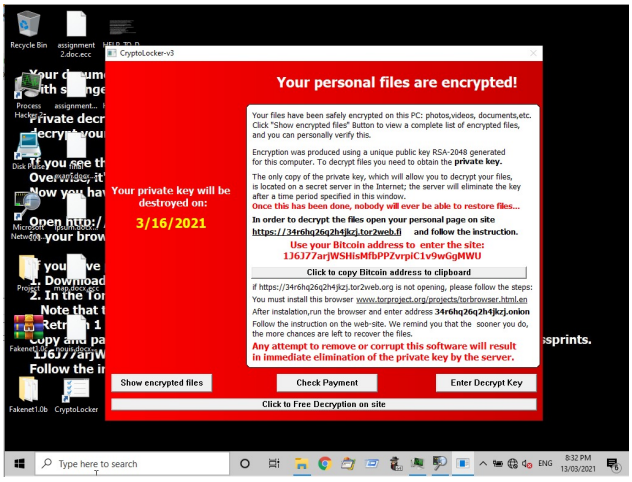

Figure 6. Ransomware sample running in Malware lab

6) Exporting the logs to host machine

Once the ransomware message popped up, all the logs were converted to a .csv file and saved on the infected machine. For safety purposes the logs were not directly transferred to the host machine. An intermediatory machine named as scanner was used to download the log files, that had an installed anti-virus (Bit-Defender) to scan the log files for any malicious content. Secure Copy Protocol (SCP) was used to copy the .csv file to the scanner machine and finally to the host machine.

Command: scp [OPTION] [user@]SRC_HOST:]file1 [user@]DEST_HOST:]file2

B. Preparing Datasets

To prepare uninfected dataset, logs from victim machine were taken before infecting it with ransomware and transferred to the host machine. (All the algorithms were run on host machine) The dataset that contained the log files from an uninfected machine was labelled as 0 and the dataset that contained the logs from infected machine was labelled as 1. Each dataset contains eight columns namely: ‘Time of Day’, ‘Process Name’, ‘PID’, ‘Operation’, ‘Path’, ‘Detail’ and ‘Class’. As PID is the process ID and is unique to each process name, the column process name was dropped from the data frame.

As machine learning algorithms require the cell values to be integer, it was required to allocate unique value to each cell in a column. To allocate unique value to cells a python code was written that can give unique value to each cell by making a dictionary from a column of the given dataset. The python code which is used to give unique value to each cell can be found at the GitHub link given in next sub section. After preparing the dataset three supervised machine learning algorithms were trained that have been discussed in the next section.

C. Running supervised machine learning algorithms

Full code for the following algorithms can be found at https://github.com/IamSachinMalik/Ransomware_Detection. Three machine learning algorithms namely Naïve Bayes, Decision Tree and Random Forest Classifier were trained using the datasets. The data was split into ratio of 80 and 20. Eighty percent of the data set was used to train the decision tree classifier model and twenty percent of the dataset was used to test the accuracy of the model.

5. Results And Discussion

All three models were trained, and the datasets were split in training and testing sets (80:20) as discussed in previous chapter. Figure 7 shows the accuracy score of each model that was trained. It can be seen in the below figure, that decision tree and random forest classifiers gave quite similar accuracy score whereas naïve bayes accuracy score is very low comparatively. After finding the accuracy score of all the models, features that were considered important by the models were considered.

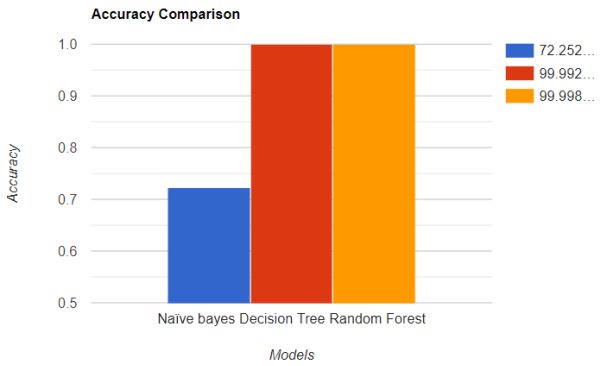

Figure 7. Accuracy Comparison between Naïve Bayes, Decision Tree and Random Forest Classifier

Though there are numerous features and activities like network traffic, entropy change in files, memory usage etc., that can be tracked on a victim machine, to restrict the

scope of this research only limited number of features were considered as shown in Table 1. These are the fundamental features that show the changes made by an application on a machine and can be used to discover more changes if studied in detail. The features considered to find the accuracy from each machine learning algorithm are as follows:

A. Process ID: This is the ID assigned to each application which is running on the windows system.
B. Time: This is the recorded time of changes that the applications are making to the system.
C. Operation: This is the task the application is doing in systems. For example: creating new file or deleting a file.
D. Path: This is the exact location where the operation is being done.
E. Result: This is the outcome of the operation performed by the application.
F. Details: These are more details about the operation being performed.

According to Table 1, it can be said that the most important feature of the data set was the process ID followed by the details of action that the program was doing in the background. It can be seen that though the Result feature has the least importance in both the classifiers, but the Decision Tree Classifier has given close to zero importance for the results whereas Random Forest classifier gave it more importance. Reason for this can be the fact that random forest consists of huge number of decision trees that works as an ensemble, and it is possible that in multiple decision trees the results feature came out to be important. The exact importance values are given in the Table 1.

TABLE I. Comparison of feature importance of random forest and decision tree classifier

Feature	Random Forest	Decision Tree
Process ID	0.369896	0.504932
Time	0.154037	0.159560
Operation	0.099509	0.036057
Path	0.091501	0.036905
Result	0.006343	0.000631
Details	0.278713	0.261915

As naïve bayes algorithm determines the unconditional and conditional probabilities related to the feature and then predict the class with highest probability, GaussianNB (variation of Naïve Bayes that follows Gaussian distribution and works with continuous data) does not have any congenital method to find feature importance. Therefore, to analyse the trained model a method known as Permutation Importance was used. Table 2 shows the permutation importance in training set and testing set that were obtained from the model trained using naïve bayes algorithm.

A convention in scikit-learn states that higher return values have better permutation importance than lower return values [24], therefore the features having higher value are more important. It can be seen that according to trained naïve bayes model "Time" was the most important feature in the log files followed by "Process ID" and the least important feature was the "Details" present in the log files.

TABLE II. Comparison of feature importance of random forest and decision tree classifier

Feature	Permutation Importance	
	Training Set	Testing Set
Process ID	0.01146765	0.01171582
Time	0.07936673	0.07913299
Operation	0.00483536	0.00529719
Path	-0.00374041	-0.00292091
Result	-0.00223502	-0.0022052
Details	-0.01335463	-0.01295968

Findings

Accuracy of Decision Tree and Random Forest algorithms is better than Naïve bayes while training models using the log files.
Process ID i.e., ID of the program running and Details i.e., what the program is doing in the background are the deciding factors to classify it as a malicious or benign program.
Result of the executed task by a program does not help in detecting the ransomware.

6. Conclusion and Future Work

Ransomware is evolving at an alarming rate, with new features in every ransomware strain that is detected. It has come a long way since it was discovered and changed its method of simply locking the victim's device to encrypting files using complex encryption algorithms. It is crucial that the detection methods adopt new methods of heuristic-based detection rather than relying on the previous signature-based detection methods as ransomware strains have been seen to use polymorphic techniques to evade the signature-based detection. This paper focused on the machine learning algorithms that uses behavioral based detection and the features that are most important in detection of ransomware based on the log files.

Based on the experiments performed during this research we can conclude that the process i.e., Process ID and its action i.e., Details are the most important features in a log file that contribute most to detect a ransomware. Whereas result of the executed tasks by a program does not play any role in detecting the presence of ransomware. Moreover, time can be one of the crucial features using which a sequence of events can be mapped thus classifying a program to be malicious or benign.

This paper only targeted a small portion of how machine learning can be used to detect ransomware attacks and what features should be given priority when classifying a malware to be ransomware. Needless to say, the technical

aspects of this paper are not flawless, and the models can be improved over time. Finally, it is not a matter of ”if” but a matter of ”when” an attack will happen therefore it is important to be prepared.

7. Acknowledgment

This research was supported by Charles Darwin University. We thank our colleagues from Charles Darwin University who provided insight and expertise that has help this research a lot.

We would also like to thank people who have indirectly helped in this research by sharing their ideas via papers and articles.

References

1) Chittooparambil, H.J., et al. A Review of Ransomware Families and Detection Methods. 2019. Cham: Springer International Publishing.
2) Kharraz, A., et al., Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. 2015. 3-24.
3) Sgandurra, D., et al., Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection. 2016.
4) Cartwright, A. and E. Cartwright, Ransomware and Reputation. Games, 2019. 10(2): p. 26.
5) Meland, P.H., Y.F.F. Bayoumy, and G. Sindre, The Ransomware-as-a-Service economy within the darknet. Computers & Security, 2020. 92: p. 101762
6) Coverware, Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020. 2020.
7) Goldsborough, R., The increasing threat of ransomware Teacher Librarian, 45(1), 61, 2017.
8) Y. Connolly, L. and D.S. Wall, The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers & Security, 2019. 87: p. 101568.
9) Kane, P.O., S. Sezer, and D. Carlin, Evolution of ransomware. IET Networks, 2018. 7(5): p. 321-327
10) Roberts, N., Ransomware: An Evolving Threat. 2018.
11) Kelion, L. Cryptolocker ransomware has ’infected about 250,000 PCs’. 2013 08/08/2020]; Available from: https://www.bbc.com/news/technology-25506020
12) Yaqoob, I., et al., The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 2017. 129: p. 444-458
13) Herrera Silva, J.A., et al., A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters. Remote Sensing, 2019. 11: p. 1168
14) SecurityPrimer, Eternal Blue. MS-ISAC, 2019. SP2019-0101
15) Bonde, S.Y. and U.S. Bhadade. Analysis of Encryption Algorithms (RSA, SRNN and 2 Key Pair) for Information Security. in 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA). 2017
16) Berrueta, E., et al., A Survey on Detection Techniques for Cryptographic Ransomware. IEEE Access, 2019. PP: p. 1-1
17) Tatam, M., et al., A review of threat modelling approaches for APT-style attacks. Heliyon, 2021. 7(1): p. e05969
18) Gupta, M., S. Mittal, and M. Abdelsalam, AI assisted Malware Analysis: A Course for Next Generation Cybersecurity Workforce. 2020
19) Hwang, J., et al., Two-Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques. Wireless Personal Communications, 2020. 112: p. 1-13
20) Kirda, E. UNVEIL: A large-scale, automated approach to detecting ransomware (keynote). in 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER). 2017
21) Mehnaz, S., A. Mudgerikar, and E. Bertino, RWGuard: A Real-Time Detection System Against Cryptographic Ransomware: 21st International Symposium, RAID 2018, Heraklion, Crete, Greece, September 10-12, 2018, Proceedings. 2018. p. 114-136
22) Lee, K., S. Lee, and K. Yim, Machine Learning based File Entropy Analysis for Ransomware Detection in Backup Systems. IEEE Access, 2019. PP: p. 1-1
23) Abukar, Y., B. Koçer, and B. Al-rimy, Automated Analysis Approach for the Detection of High Survivable Ransomware. KSII Transactions on Internet and Information Systems, 2020. 14: p. 2236
24) Breiman, L., Random Forests. Machine Learning, 2001. 45(1): p. 5-32

8. About Authors

Sachin Malik works as a Graduate ICT Specialist, where he regularly practices his scripting and secure programming skills. He is passionate about finding bugs in applications to make them secure from adversaries. Sachin completed a Master in Information Technology with a major in Cyber Security from Charles Darwin University. In his studies, he focused on various offensive and defensive techniques that can be used to test the security stance of a network infrastructure.

Bharanidharan Shanmugam is currently a research-intensive Senior Lecturer with the College of Engineering and IT, Charles Darwin University, Australia and Darwin branch chair of Australia Information Security Association. He has a large number of publications in several different journals and conference proceedings. His research interest mainly revolves around the field of cybersecurity and he is keen in nourishing the cyber skills of next generation.

Krishnan Kannoorpatti is currently a Research Active Associate Professor with the College of Engineering, IT and Environment, Charles Darwin University, Australia. In addition of being a stellar academic and innovative researcher, he also has an extensive experience of working with the government bodies in setting up data privacy policies at national and state level.

Sami Azam is currently a senior lecturer and researcher with the College of Engineering and IT, Charles Darwin University, Australia. His research expertise includes machine learning, artificial intelligence, deep learning, advanced signal processing and image analysis. He has also applied machine learning and other artificial intelligence techniques to detect and classify a range of cyber security threats.