International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Ransomware Automatic Data Recognition Tool using SRANSAC

M. Manoj, Rani V. G.

Abstract: ***In recent times, Ransomware is the most common form of malware seen which are achieved through ransomware attacks. The most common attacks are DDoS, Malicious Insiders, and Phishing. In this research work, information related to the ransomware attacks on windows and Linux are extracted, the detection of OCR(Optical character recognition) is improved to generate the screenshot of the infected machine and corresponding information are added to the database so that patterns are enhanced. The Hybrid Speeded Up Robust Feature (SURF) algorithm and image matching using Random Sample Consensus (SRANSAC) algorithm, bundle adjustment and image blending algorithms are used to develop the proposed model. An additional step is taken to crop the dark surrounding areas in the stitched image. Frequently used ransomware are crysis,gandcrab, crypto jacking and Notpetya. If the ransomware attack is detected in online data then the stored results is implemented so that USB dependence is avoided and to safeguard from the Ransomware like Crysis or GandCrab. Research work also focuses in developing online storage process.***

Key words: ***OCR, SURF, Crysis, Gandcrab, Notpetya and Cryptojacking.***

I. INTRODUCTION

Ransomware plays a vital role in malwares. Many users, institutions and organizations were threatened by ransomware which leads to major financial and reputation loss. So, it is important to design a tool which detects and prevents ransomware efficiently and effectively considering the various parameters like minimum error rate, lower costs etc.

The main knowledge of the ransomware stages used in this model are achieved from

Study of 18 ransomware methods in Windows application for deployment. The Programming Interface (API) functions were called during each ransomware execution. The research also focus on querying and interviewing ransomware victims which helps in locating common factors between the attacks in higher levels.

The attacker uses strong encryption algorithms to encrypt the files so that the user need to pay the ransom within the specified of period to access the encrypted files. If not paid then user may not able to access the files in the computer's screen [1]. Recently ransomware has been widely used to target the computers with the addition of new malwares. Ransomware reaches the target computer using some social engineering techniques that are activated when the user downloads the e-mail attachments or clicks on insecure links. Since ransomware spreads over the network easily, the numbers of victims are high in number. Ransomware easily hides the location on reaching the target with the help of jump point's detection and hence detecting becomes very difficult. The ransomware encrypts the most commonly used files in the target computer and therefore it is essential for the individual users or institutions to pay a ransom for decryption [2]. Attackers nowadays prefer Bitcoin, an anonymous payment mechanism for payment and thereby concealing their identity and location. These irregularities encourage attackers to select ransomware when compared with other malware for malicious attacks.

The software utilizes image process so that the texts are extracted from the messaged that are pops up. The text which is extracted is automatically checked to remove the errors with the help of OCR. The quality of the scanned image is analyzed by image dataset. The tool extracts and classifies the text which helps in generating the screenshot of the attacked machine.

II. LITERATURE REVIEW

A. Petya Ransomware Attack

Most common ransomware attacks in recent times are the Petya ransomware attack. The methodology and threats to Petya ransomware are discussed. The author Jagmeet Singh Aidan aids in discussing the awareness and Mitigation for the ransomware [3]. the attack may get started through the phishing e-mail and expected to have malicious code. The attack is occurred when the victim access the attachment from the mail or opens it and then the malicious code is automatically accessed [10].Prevention techniques and patch for the Petya Ransomware are given, so that the attack can be prevented beforehand by detecting and recovering of the files back. System will be highly protected and saved from being encrypted.

B. Ransomware Threat Hunting and Intelligence

Ransomware samples and 572 samples of TeslaCrypt [4] ransomware were used by the researcher .

Manuscript published on January 30, 2020.
* Correspondence Author
M. Manoj*, Assistant Professor, Department of Computer Science, Angappa College of Arts and Science, Seerapalayam, Coimbatore, India.
E-mail: manomca24@gmail.com
Dr. RaniV. G., Associate Professor, Department of Computer Science Sri Ramakrishna College of Arts and Science for Women, Coimbatore, India.

Sajad Homayoun, and Ali Dehghantanh employed Sequential Pattern Mining so that Maximal Frequent Patterns (MFP) is used with wide features to classify using J48, Random Forest Bagging and MLP algorithms [6]. It was found that the system achieved 99% of accuracy when samples contained ransomware and 96.5% of accuracy in detecting ransomware from the sample provided.
The results indicated that on using techniques to identify patterns leads to identification of ransomware hunting [9].

C. White List Based Ransomware

Wide range of people may become victims of new ransomware without their knowledge. For detecting abnormal behavior, the software is executed on users' devices by marking the folder as secured so that software can be controlled while accessing the files. However, such an approach may cause inconvenience to users and their corresponding behavior [5]. Hence, to detect/control ransomware effectively and securely, this paper proposes a new method to detect or block ransomware by analyzing the file operation procedure in the device where people access and also by accessing various scheme control to the file operation procedure. The authors Dae-Youb Kim and Geun-Yeong Choi proposed a real- time scheme to detect ransomware by encrypting file which is important in user's machines before displaying the information about the ransomware. As a result new ransomware can be prevented in real time.

D. Crypto Drop

In this research work, on implementing the Crypto Drop degrees of early-warning system is detected so that the system alerts the user throughout suspicious file activity. While employing a set of behavior indicators, Crypto Drop will halt a method that can meddle with huge quantity of the user's information [7]. by combining a collection of common indicators to ransomware, the system may be parameterized for the fast detection with low false positives. Nolen Scaife and Hendry rendered experimental analysis of CryptoDrop to remove from death penalty with a little loss of solely ten sets (out of nearly five, 100 obtainable files). The results indicated that careful analysis of ransomware behavior will efficiently detect the system that considerably mitigates the quantity of victim information loss.

E. Ransomware Tracer

Remote desktop protocol (RDP) threats ransomware. To overcome the issue, ZiHan Wang and Xu Wu proposed methodology using trapping and tracing to control RDP attacks. System that can traced is formed with help of cyber deception called Ransomtracer was developed [8]. RansomTracer gets the clues on the person with help of deploying monitors in the respected environment. Then, the traceable clues were automatically extracted and traced. The results relieved that Ransom Tracer increased the analysis efficiency. Then these clues are recognized to identify the attackers and 98.34% screening rate is achieved.

III. PROPOSED METHODOLOGY

In this section, the architecture of the proposed model defined in detail on several aspects
The following are the modules used in the research paper

A. Ransomware Attack
B. Hybrid random sample SURF algorithm
C. Ransomware families
D. Online data storage

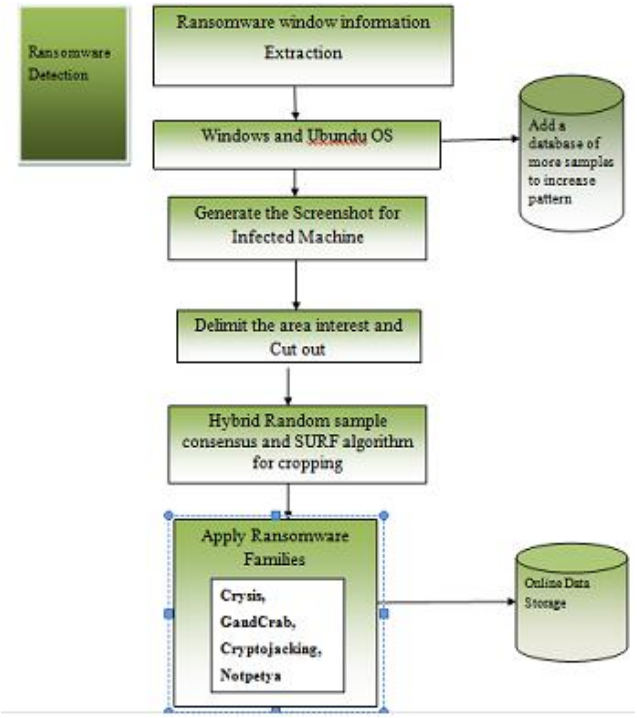

Figure 1: Proposed Diagram

A. Ransomware Attack

Ransomware is a kind of program which may affect the security of the system. Malicious code is widely used by the attackers. Information gets encrypted prior to accessing. Money is earned with help of these data. Older system doesn't help to cure corrupted system without accessing the information. The encrypted data is recovered using the encryption. Screen shots are generated for the payment in the infected system.

B. Hybrid Random Sample SURF

The machines are infected due to ransomware attacks. Optical character recognition is used to generate the screen shot for the infected system. Then the image from the given database is uploaded to the SURF algorithm for image matching. RANSAC helps the image to crop the dark surrounding area in the stitched image. The each image is examined in a sequence, as a grayscale image an obligation of SURF algorithm. SURF awareness point detector is to applied to detect the points of interest in the image. SURF descriptor is useful in extracting the detected points which may or may not return a descriptor for the intended point. SURF descriptor and the behavior of comparable descriptor are stored for further analysis.

Hybrid random sample SURF algorithm:

1. The proposed techniques were Hybrid SURF and Random Sample Consensus. Initially screens are captured and images features are extracted by using SIFT and SURF method.
2. With help of extracted feature, the necessary features are obtained by using RANSAC (Random Sample Consensus) from the original image. The RANSAC helps to remove unnecessary feature points.
3. The right feature points are associated with their corresponding feature point. Again the RANSAC is applied on these feature points to stitched image of input image.
4. Cropped image is then fetched.
5. The javaocr was applied to the cropped image and ransomware message are extracted.

A. Ransomware Families

Crysis, gandcrab and Notpetya, Ransom are applied to detect the ransom. Crysis is ransomware that encrypts files on an infected system. Ransomware is a kind of program which stops the people from using their personal files and demands the user to access using weak or leaked RDP passwords. At times malicious mail attachment or installing any game software also leads to the ransomware attacks.
Table 1 projects most delegate families which was designed over the year.

Table: 1 Ransomware Evolution

Year	Ransomware Family Discuss
2016	Crysis
2017	Notpetya
2018	Gandcrab
2018	Crypto jacking

Crysis : The ransomware encrypts all types of files, network drives, drops a copy itself in multiple registry locations for permanent storage.
Notpetya : it reboots the computer and encrypts the master boot record files. Attackers may demand Bitcoin payment so that hard drives are decrypted.
Gandcrab: It helps to encrypts the user file and demands the payment so that user can regain the access to the data.

Crypto jacking or malicious crypto mining is an upcoming online threat which hides on a computer or mobile device and access the online money resources called crypto currencies. Crypto jacking steals computing resources from their victims' devices by staying in the user's resource which also slow down the other process.

B. Online Data Storage

If the ransomware attack is detected in online data then stored results is implemented so that USB dependence is avoided and to safeguard from the Ransomware. Storage such as Cloud may safe from ransomware by backup security for Use of Encryption advantages as it's more difficult to access without proper authentication.

IV. EXPERIMENTAL RESULTS

In these experiments, the tool with all the automated functionalities was utilized to get information about ransomware and also identify the files related to the attack for the corresponding system. The machines characteristics: Intel Pentium 64-bit Architecture Processor, 4GB RAM and Windows 8 Operating System and Linux environment,

Malware Forensic Analysis

The image is assembled in a system memory. Images corner are cross checked. The correctness of analysis was ensured using the System memory acquisition. Different types of tools are experimented in this system.

Memory Dump:

Memory dump contains the working module of the memory in a particular point of time, mainly when the system terminated unexpectedly. A core dump indicates the represents the complete contents (address) regions of the process. With operating system as base the dump containing the structure to aid the interpretation of the memory regions. In these systems, the program is required for the successful interpretation or dump can be interpreted for understanding the structure of the program's memory use.

Dumpit: Memory dump tool runs easily and access the data. It executes by command line console so that the process are computerized.

RAMCapturer: a little forensic analysis tool which is allows the user to access the information from RAM.

Winpmem: This tool is an open source framework which is used to extract the volatile memory. This tool is developed using python and found in github.

FTK imager: It is virtually imagined and quick tool to get information. It's a tool commonly used to extract and analysis.

SRANSAC: It's a tool to detect ransomware attack and contains hybrid surf. Random Sample Consensus (SRANSAC) tool runs through user interaction and images are extracted for decoding.

Sample / Tool	Cerber	Locky	TeslaCrypt	Wannacry	Crysis	Notpetya	Gandcrab	Crypto jacking	Execution Time	Without user interaction
Dumpit	✓	✓	✓	✓	✓	✓	✓	✓	50	✓
RAM Capturer	✓	✓	✓	✓	✓	✓	✓	✓	58	×
FTK Imager	✓	✓	✓	✓	✓	✓	✓	✓	52	×
Winpmem	✓	✓	✓	✓	✓	✓	✓	✓	51	×
SRANSAC	✓	✓	✓	✓	✓	✓	✓	✓	48	×

Table: 3 Result for Screenshot for tests

In order to select the best memory dump tool, SRANSAC was executed on a computer which is infected with different samples of ransomware like Crysi, Notpetya, Gandgrab, cryptojacking.

The tests were conducted on a 64-bit architecture system with 4GB RAM with Windows 8 as the base operating system.

The ransomware samples were implemented and the behavior and total processing time were counted.

OCR Recognition Result

In order to find the efficiency of OCR, this functionality was apply to the pop-up windows of different types of ransomware samples,

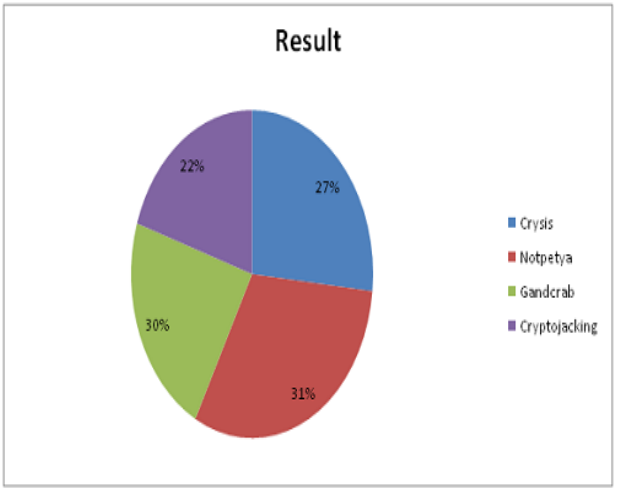

Figure 2: OCR Recognition Result

Execution Time:

Execution time mentions to the viability of SRANSAC method with respect to time required to complete the detection of Ransomware.

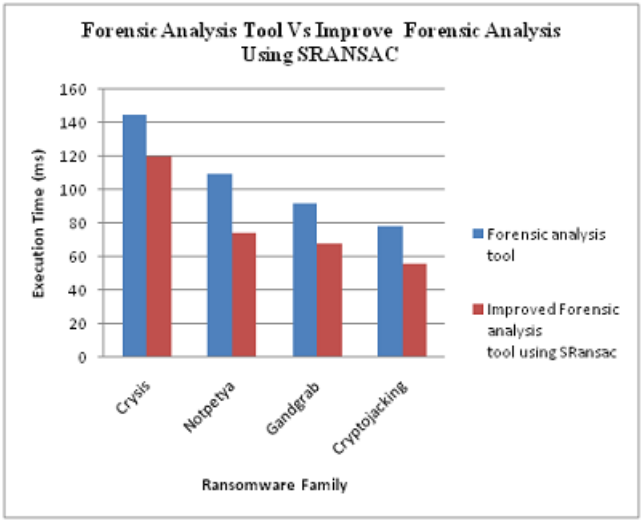

Figure 3: Execution Time for Forensic Analysis Tool Vs Improved Forensic analysis tool using SRANSAC

Ransomware Family **Execution Time(ms)**	Forensic analysis tool	Improved Forensic analysis tool using SRANSAC
Crysis	145	120
Notpetya	110	74.58
Gandgrab	92	68.25
Cryptojacking	78	56.39

Table: 4 Execution Time for Forensic Analysis Tool Vs Improved Forensic analysis tool

Memory:

Memory mentions to the viability of a SRANSAC method with respect to memory required to complete the detection of Ransomware.

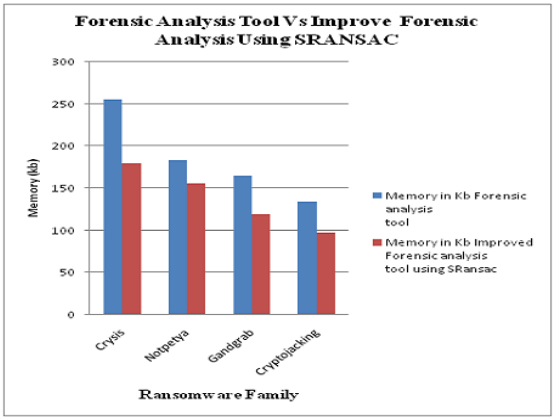

Figure 4: Memory for Forensic Analysis Tool Vs Improved Forensic analysis tool using SRANSAC

Ransomware **Memory in (Kb)**	Forensic analysis tool	Improved Forensic analysis tool using SRANSAC
Crysis	256	180
Notpetya	184	156
Gandgrab	165	119
Cryptojacking	134	98

Table 5: Memory for Forensic Analysis Tool Vs Improved Forensic analysis tool

V. CONCLUSION

The attackers never intended to give back the data or do not implement their data recovery functionality. In either case, if ransomware protection fails, both money and data are lost. Hence a model for ransomware attack was proposed using data from various analyses. The OCR capabilities extended by using Hybrid random sample SURF algorithm to get optimal performance. Different environments were used and the obtained the desired outcome. RAM memory and USB speed determine the runtime. Tool was further explored based on the performance in other machines with different operating systems. Dumped data analysis could be enhanced by using the timestamp of the files.

REFERENCES

1. Kharraz A, Robertson W, Balzarotti D, et al. Cutting the Gordian Knot: A Look under the Hood of Ransomware Attacks [J]. Lecture Notes in Computer Science, 2015, 9148:3-24.
2. Mohurle S, Patil M. A brief study of Wannacry Threat: Ransomware Attack, International Journal, 2017, 8(5)
3. Jagmeet Singh Aidan.Survey on Petya Ransomware Attack, International Conference on Next Generation Computing and Information Systems, 2017
4. A. Azmoodeh, A. Dehghantanha, M. Conti, and R. Choo, "Detecting crypto-ransomware in iot networks based on energy consumption footprint," Journal of Ambient Intelligence and Humanized Computing, 2017.
5. Dae-Youb Kim and Geun-Yeong Choi, "White List-based Ransomware Real-time Detection and Prevention for User Device Protection", IEEE International Conference on Consumer Electronics,2018.
6. M. Sun, X. Li, J. C. S. Lui, R. T. B. Ma, and Z. Liang, "Monet:A user-oriented behavior-based malware variants detection system for android," IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, pp. 1103–1112, may 2017
7. MattiasWeckstén, Jan Frick, Andreas Sjöström, Eric Jarpe, "A novel method for recovery from Crypto Ransomware infections", Computer and Communications (ICCC), 2016 2nd IEEE International Conference.
8. ZiHan Wang and Xuwu "RansomTracer: Exploiting Cyber Deception for Ransomware Tracing", IEEE Third International Conference on Data Science in Cyberspace,2018.
9. Hajredin Daku, Pavol Zavarsky, "Behavioral-Based Classification and Identification of Ransomware Variants Using Machine Learning",IEEE International Conference On Trust, Security And Privacy In Computing And Communications, 2018.
10. S. Kok, A. Abdullah, M. Supramaniam, T. R. Pillai, and I. A. T. Hashem, "A Comparison of Various Machine Learning Algorithms in a Distributed Denial of Service Intrusion," Int. J. Eng. Res. Technol., vol. 12, no. 1, pp. 1–7, 2019.

AUTHORS PROFILE

Manoj M., Assistant Professor, Department of Computer Science, Angappa College of Arts and Science, Seerapalayam, Coimbatore India, Email: manomca24@gmail.com

Dr. Rani V. G., Associate Professor, Department of Computer Science Sri Ramakrishna College of Arts and Science for Women, Coimbatore, Coimbatore India.