RANSOMWARE ATTACK DETECTION USING IMPROVE TIMESTAMP AND DATABASE

M.MANOJ, MCA., M.Phil(CS).,(Ph.D).,

1. Assistant Professor, Department of Computer Science, Angappa College of Arts and Science, Seerapalayam, Coimbatore India.

Email: manomca24@gmail.com

Dr.Rani.V.G

2. Associate Professor, Department of Computer Science, Sri Ramakrishna College of Arts and Science for Women, Coimbatore, Coimbatore India.

ABSTRACT

Ransomware is a particular category of malicious software that aims to encrypt the data of the infected users, making them unusable, and asking for a ransom in exchange for the decryption keys necessary to restore them. The attacks have become increasingly refined and difficult to counter, to the point that, even considering the different solutions designed against this threat, damage remains considerable, and ransomware keeps spreading. The proposed work is focused on this last aspect of the researching an attempt to provide more in-depth information useful for studying the ecosystem behind the attacks, we have developed anti-ransom tool, a framework for fully automated extraction of data from ransomware samples. By running the samples in a monitored environment and collecting the artifacts left in the system at the end of the malicious activity The tool perform the image processing to extracted the text in the popup message the extracted text is automatically corrected remove the errors through the OCR (Optical character Recognition) The anti-ransom tool, which detects and prevents ransomware on machines other operating system supported and memory dump improved the time stamp of the files.

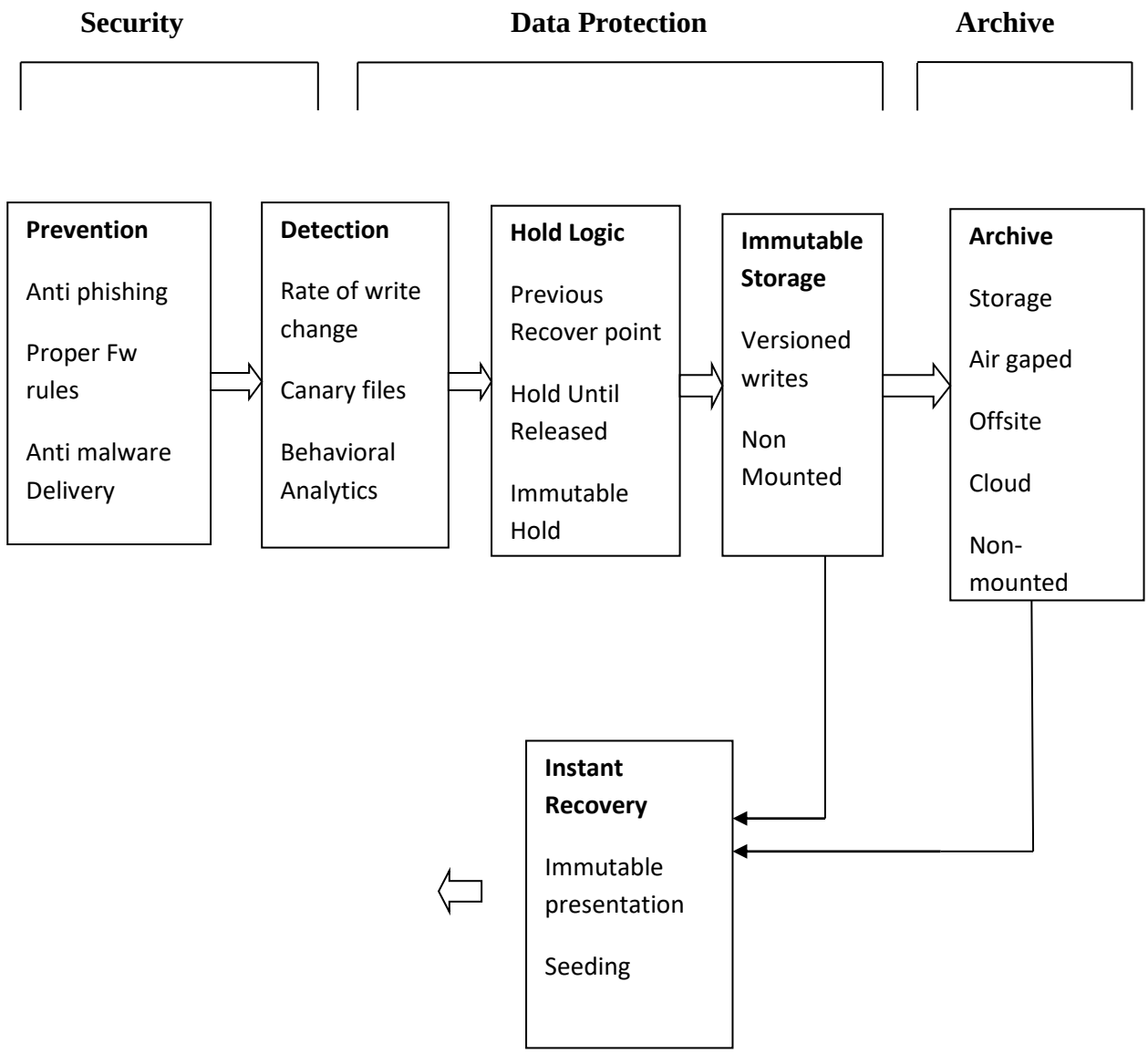
Keywords: Anti-ransom tool, OCR, Memory dump, Timestamp

I. INTRODUCTION

Ransomware is a form of malware that extortion to the victim. The name ransomware comes from the ransom note asking its victim to pay some money in return for gaining back access to their data or device, or for the attacker not to divulge the victim's embarrassing or compromising information. It spreads through malicious e-mail attachments, infected software apps, infected external storage devices or compromised websites. [1]Unlike other types of malware, ransomware exposes itself at some stage of its execution in order to deliver the ransom demand to its victim. This demand is presented with a note that appears on the screen before or after the encryption occurs, outlining the threat and accompanied by a detailed set of instructions for making the payment, typically through a cryptocurrency.

Since ransomware hides its location once it reaches to the target through jump points, detecting an attack becomes extremely difficult. The ransomware encrypts the most commonly used files in the target computer individual users or even institutions are forced to pay a ransom for decryption. Attackers prefer Bitcoin, an anonymous payment mechanism, as a means for payment, thereby concealing their identity and location. [2]

This approach is to let the ransomware sample run in a controlled environment, then collect artifacts left from the execution, such as files, screenshot of the desktop of the emulated machine, memory dump, and examine the information left in order to find information useful for understanding the ransomware background and perform investigation (e.g. payment addresses, email accounts, URLs of malicious websites). Given the multiplicity of different sources of information analyzed, it is impossible to treat every source in the same way. The tool performs the image processing to extract the text in the popup message the extracted text is automatically corrected to remove the errors through the OCR. [3] The image dataset analyzed the quality of the scanned image. The tool extracted and classified the text is threatening to generate the screenshot of the attacked machine. The anti-ransom tool detects and prevents ransomware on machines with Windows OSs. Our study utilized many academic publications, reports of leading international cybersecurity companies, and interviews with many cybersecurity experts. The finding from windows OS and Kali Linux. [10] We proposed other operating system supported and improved the time stamp of the files



Anti- Ransomware Architecture

II. LITERATURE REVIEW

Ransomware Attacks Prevention, Monitoring and Damage Control

Ransomware is sort of malware that forestalls or restricts user from accessing their system, either by locking the systems screen or by locking the user's files within the system otherwise a ransom paid. Anti-Ransomware software applications are designed to run within the background and block attempts by Ransomware to encrypt data. it's also monitor the Windows registry for text strings known to be related to Ransomware More modern ransomware

families, individually categorize as crypto-ransomware, the author Jinal P. Tailor Ashish D. Patel encrypt certain file types on infected systems and forces users to pay the ransom through online payment methods to urge a decrypt key. [4] The analysis has been a big improvement in encryption techniques employed by ransomware. The careful analysis of ransomware behavior can produce an efficient detection system that significantly reduces the quantity of victim data loss.

Malware Threats Faced by the Typical Email User

The propose administered on spam email data received by one user test email account collected over a period of six months. Analysis of email data using the sandbox setup helps to supply a comprehensive data analysis about botnet behavior. The author Anthony Ayodele, James Henrydoss described intimately the planning and implementation of the sandbox test environment including the challenges faced in building this test environment. It's used VMware based virtual platforms built on Linux PC-class hardware. [5] We present the results of our behavioral measurement of the foremost active botnets. The study found that for one email user for a period of six months, two active Trojans contributed around 20 percent of the entire identified malware received within this point period and therefore the remaining 80 percent of malware binaries were distributed over many various sorts of botnets the e-mail malware shows a classic long-tail distribution.

Ransomware attack

The first of this malware made intense use of cryptography, specifically for file encryption. They encrypt some or most files on the pc before asking a ransom for the decryption. Since they appeared, however, Ransomware has evolved into differing types which fulfill their task in several ways. The author Mihail Anghel, and Andrei Racautanu Some encrypt files and data from the disk drive, others block access to the OS or use private user data to blackmail the user, some aren't even a true threat, but they scare the user into paying for a few fake service or software. The software security industry is cognizant of those threats and is consistently analyzing the new versions and kinds to work out how dangerous they're and to supply an updated protection solution. This text tries to research and compare the way this malware works and the way they affect the victim's computer. [8] Our analysis will provide a stimulating insight into how they work it'll highlight the particularities of Ransomware and

can give some information about why a number of these malware are more dangerous than others.

Detection and Avoidance of Ransomware

Ransomware may be a sort of malware that stops or limits users from accessing their system, either by securing the screen of the system or by locking the user's files unless a ransom is paid. it is important to design a tool that detects and prevents ransomware efficiently with the minimum false positive and lower costs.Hindering of ransomware is important so as to save lots of the user's file. The author S.Mahmudha Fasheem, and P.Kanimozhi propose the automated test packet generation (ATPG). it's maybe a model that's wont to produce a minimum set of test packs to exercise each link within the network. [6]Test packets are sent occasionally and detected failures prompt a definite mechanism to localize the fault. ATPG reads a router configuration and creates a device independent model. This prevents the ransomware from entering the system.

The Successful Ransomware Prevention Technique Using Process Monitoring on Android

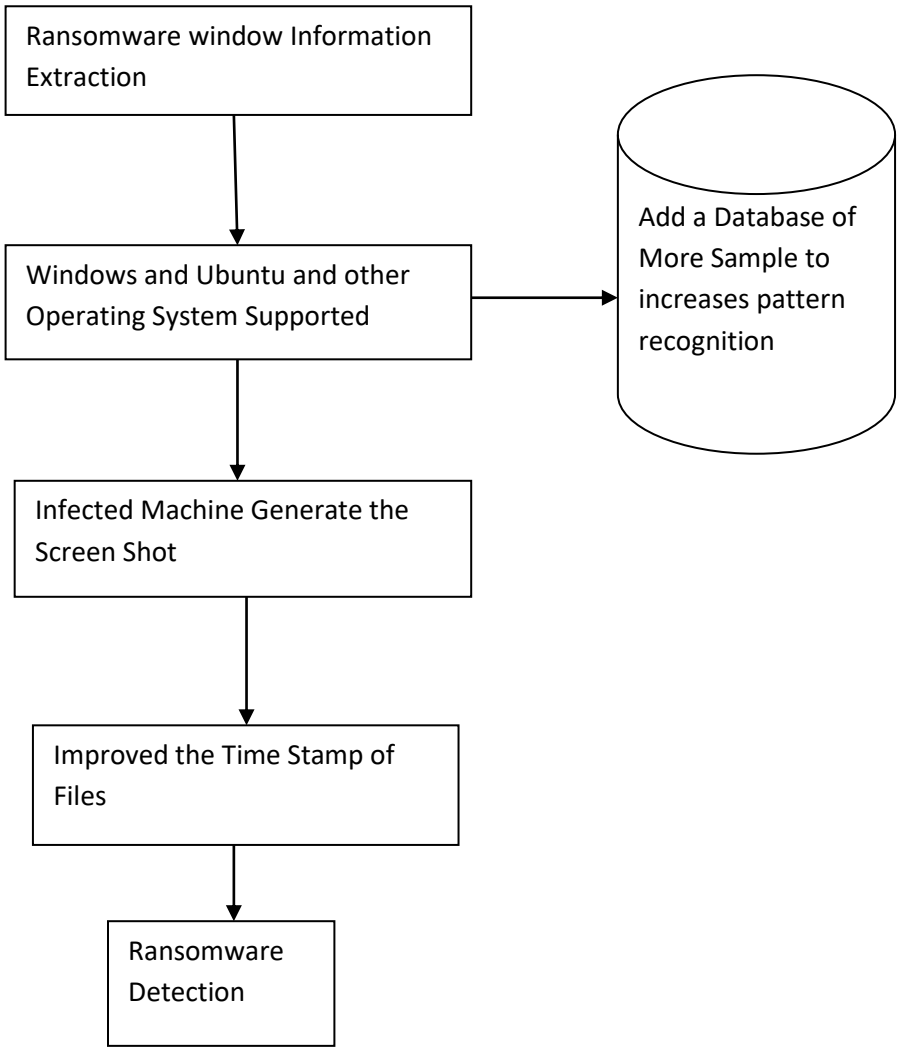
The attacks of ransomware, damage cases including encryption of users' important files are constantly increasing. the prevailing vaccine systems are susceptible to attacks of latest pattern ransomware because they will only detect the ransomware of existing patterns. A simpler technique is required to stop modified Ransomware. Proposed technique is supposed with three modules configuration, monitoring, and processing configuration module generate a monitoring list table for a smooth operation of the proposed method. [7] It's the module for the initial setting. The monitoring module is liable for monitoring Processor, Memory, and Storage I/O usage of each process in real-time supported statistical techniques. Finally, the method module determines the handling of the process suspected as ransomware by the Monitoring module and makes an exception or isolation of the process.

Extracting Intelligence from Ransomware Families

The lack of ties between ransomware attacks and real people is not an unfamiliar problem and since the ransomware explosion many approaches to fill this knowledge gap have been studied. The most relevant and comprehensive is the tracking of ransomware payments end-to-end conducted by Google They conducted a study lasted two years and similar to the one showed

here. They collected information on infected machines in order to find the BitCoin address showed for payment, and used it to trace ransoms on the BitCoin network. The differences between their study and ours are many they focused mainly on the tracing part, and their information collection was limited to wallets address search. [9] We focused instead on the collection and extraction part, not limiting ourselves to wallets but extracting all kind of interesting information left by the malware, specifically focusing on everything that could be helpful for intelligence. After that, while they focused only on certain ransomware families, we tried to maintain a high level of generalization, in order to design an approach valid in all cases, making the resulting framework useful for all kind of samples, even for future ones.

III. METHODOLOGY



MODULES

1. Ransom Information Extraction
2. Database of More Samples added
3. Other Operating System supported
4. Improved Timestamp of Files

Ransom Information Extraction

The tool runs once the computer has been infected, must be able to perform a full memory dump of the affected system and at the same time perform a screenshot that allows you to obtain the additional information mentioned above for use in the classification and correlation of malware. Extract information from the ransomware pop-up window from the infected device.

Database of More Sample Added

The collect data left from ransomware execution from the different sources files created or modified, screenshots taken during execution, memory dump of the process, network traffic. Files created are collected using the agent controlling the tool that transfers all new files via networking to a dedicated folder. The agent can also control the desktop content in order to take the screenshots, we collects the memory dump that saved in end of the process execution

Operating System Supported

The tool perform the image processing to extracted the text in the popup message the extracted text is automatically corrected remove the errors through the OCR. The image dataset analyzed the quality of the scanned image. The tool extracted and classified the text the text is threatening generate the screenshot of the attacked machine. The ransom tool which detects and prevents ransomware on machines with a version of the tool that works on other operating systems.

Improved Timestamp of Files

We extract the memory dumps coming from malware execution, decoding them, and searching in them for strings composed of more than four readable characters. We then operate a differential analysis comparing the strings found in this way with the ones extracted in this same way from the baseline dump. In this way we can filter out information present on the memory by default and select almost only relevant information, left on the system by the malicious process the analysis of the data dumped from memory could be improved the time stamp of files.

Improve Timestamp and add More Samples in database in Ransomware:

1. The 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.
6. The captured image samples are stored in database.
7. The captured image files are stored in Memory using Timestamp and get processing time.
8. Using timestamp reduce the processing time .

IV. RESULT AND DISCUSSION

No. Of Files dumped Memory	With Time Stamp(Seconds)	Without Time Stamp (Seconds)
100	10	100
200	20	150
300	30	200
400	40	350
500	50	500

Table: Number of files dumped in memory time Stamp

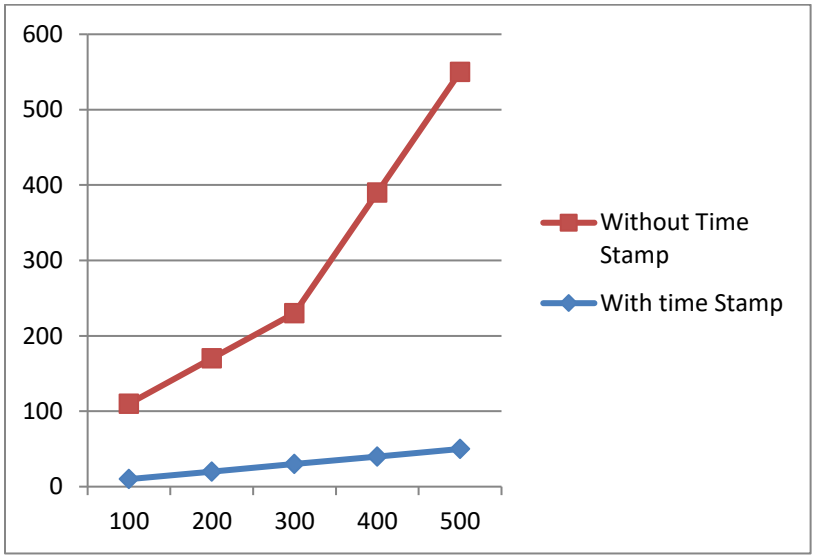


Fig: Memory dumped in Time stamp

CONCLUSION

Ransomware Detection and Prevention Tool which is aiming to detect and prevent ransomware at the OS level, network traffic analysis .In this work the search for patterns in images was carried out in order to obtain sufficient information to determine. a database of more samples to increase pattern recognition and monitoring the OS processes, services, registry records, as well as behaviors on the file system are controlled. Implement online storage of results to avoid dependence on USB and protect the tool against ransomware such as Crysis or GrandCab. The possibility of a version of the tool that works on other operating systems. It was concluded that the tool has an optimal performance, in the different environments that was executed obtaining the expected results.

REFERENCE

1. N. A. S. Z. C. Zheng, N. Dellarocca and F. Maggi, “Greateatlon: fast, static detection of mobile ransomware,” in Proceedings of the International Conference on Security and Privacy in Communication Systems, 2016, pp.617–636.

2. P. H. Rughani, “Formality: Automated forensic malware analysis using volatility,” International Journal of Advanced Research in Computer Science, vol. 8, no. 3, 2017.

3. T. Y. Z. L. Jing Li, Congcong Li, “Cross-domain co-occurring feature for visible infrared image matching,” IEEE Access, vol. 6, pp. 17 681 –17 698, 2018.

4. Jinal P. Tailor Ashish D. Patel, “Ransomware Attacks Prevention, Monitoring and Damage Control”, International Journal of Research and Scientific Innovation, vol. 4, no 6, 2017.
5. Anthony Ayodele, James Henrydoss, “Malware Threats Faced by the Typical Email User”, Springer-Verlag Berlin Heidelberg, pp. 513–525, 2011.

6. S.Mahmudha Fasheem, P.Kanimozhi, “Detection and Avoidance of Ransomware”, International Journal of Engineering Development and Research, vol 5, Issue 1 2017.

7. Sanggeun Song, Bongjoon Kim, “Ransomware Prevention Technique Using Process Monitoring on Android”, Research Article 2016.

8. Baris Celiktas, Ertugrul Karacuha, “Ransomware, Detection and Prevention Techniques”, https://www.researchgate.net
9. Sajad Homayoun, Ali Dehghantanha, “Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence”, IEEE Transactions On Emerging Topics In Computing,2017.
10. Muhammad Nur Faiz, Wahyu Adi Prabowo, “Comparison of Acquisition Software for Digital Forensics Purposes”, https://researchgate.net