OPEN ACCESS
ISSN 2356-5462
http://socj.telkomuniversity.ac.id/ijoict/

Intl. Journal on ICT
Vol. 10, No. 1, Jun 2024. pp. 90-99
doi: doi.org/10.21108/ijoict.v10i1.940

# Comparative Impact Analysis of Ransomware using Dynamic Analysis Techniques on Windows 10

Christopher Arden Anugerah [1], Niken Dwi Wahyu Cahyani [2*], Erwid Musthofa Jadied [3]

[1,2,3]*Informatics Faculty, Telkom University*
*Jl. Telekomunikasi. 1, Terusan Buahbatu - Bojongsoang, Telkom University, Sukapura, Kec. Dayeuhkolot, Kabupaten Bandung, Jawa Barat, Indonesia*

[*] nikencahyani@telkomuniversity.ac.id

**Abstract**

Malware, short for malicious software, is software or code specifically designed to damage, disrupt computer systems, or gain unauthorized access to sensitive information. Based on type classification, one of the well-known types of malware is ransomware. Usually, ransomware will encrypt the files on a computer system and then demand a ransom from the owner of the computer system so that the owner can regain access to the encrypted files. Sometimes in some cases, ransomware is able to delete files without input from the computer system owner. This research only uses dynamic analysis approach on the analysis process of three ransomware samples that are known for successfully causing losses to many computer systems throughout the world, namely WannaCry, Locky, and Jigsaw. It utilizes Process Monitor and x64dbg to track the processes carried out by the ransomwares. The purpose of this research is to determine which of the three samples has the highest to lowest damage level using metrics that are based on deletion attack structure and cryptographic attack structure. The findings of this research indicate that WannaCry has the highest damage level followed by Locky and then Jigsaw.

**Keywords:** cryptographic attack, deletion attack, dynamic analysis, Jigsaw, Locky, malware impact, ransomware, WannaCry

## I. INTRODUCTION

Over the past few years, the development of the internet usage has grown drastically. It has affected the way people communicate, money transaction, and also business marketing. All of those sectors are now tied to internet connection to stay relevant [1]. Other than the positive side of internet development, there is also the negative side. People became more creative on building powerful malwares that can target the victim's machine and take control over it remotely. This occurrence made malware attacks more common than before [2], [3], [4].

The goal of malware attacks has expanded to achieve something much more profitable in this modern world, such as money, intelligence, and power [5]. One of malware variants known as ransomware can encrypt victims' files and demand a ransom for their release. This type of malware has had a significant financial impact across various sectors, including healthcare, education, and government. Therefore, an optimal method is needed to analyze ransomware attacks. By analyzing ransomware attacks, we can understand how ransomware works,

Received on 31 May 2024. Revised on 29 June 2024. Accepted and Published on 30 June 2024.

what it does, and how to create an effective defense strategy for it. Additionally, it can expose the motives and methods of the attackers, providing valuable information for law enforcement agencies [3], [4]. Detecting ransomware early and preventing it from executing its harmful code is vital to combating these attacks [2].

Complete analysis of ransomware can be difficult and very demanding to do. The time commitment is key to do a very thorough analysis. Not to mention, advanced skills in cybersecurity, programming, and reverse engineering are also essential for a complete analysis towards ransomware. Additionally, the analysis also costs a considerable amount of money for the tools and software licenses. This situation is problematic because ransomware continues to evolve stronger to combat even the most robust protection yet on computers. Thus, it is necessary to find a faster way to analyze ransomware that can give results that are at least almost as accurate as the results obtained from complete ransomware analysis.

One effective method for analyzing ransomware is dynamic analysis. This process is carried out on a virtual machine, ensuring that the infected files are examined in an environment hidden from the ransomware, as some ransomware employs anti-virtual machine and anti-emulator techniques [1]. In dynamic malware analysis, the ransomware is executed in a controlled environment to safely observe its behavior. This analysis utilizes various controlled environments, such as emulators, debuggers, simulators, and virtual machines [2], [5]. By using dynamic analysis approach, we can cutout the time needed for the analysis and lower the cost while still getting accurate results of the impact of ransomware attacks.

The goal of this research is to use dynamic analysis approach to help categorize ransomware based on the impacts of the attack. However, the research is limited only to the Microsoft Windows 10 Operating System and with three samples of ransomware consisting of WannaCry, Locky, and Jigsaw. We use Windows 10 Operating System because it is the most recent major Windows Operating System, making our research more relevant for current and future interests [12]. All three ransomware samples are also chosen because of their popularity in ransomware attacks occurrence [16]. In order to analyze them, we use VirtualBox and analyzing tools such as x64dbg and Process Monitor. VirtualBox is an open-source hypervisor developed by Oracle that is available for many operating systems, x64dbg is a program that observes and examines the execution of other program, and Process Monitor is a monitoring software developed for Windows and Linux [3], [12].

## II. LITERATURE REVIEW

### *A. Malware*

Malware or also known as Malicious Software is a software that executes malicious content on computers, cellphones, networks and others. Malware has various types and each type has the same goal, namely affecting the victim's system in various ways such as damaging the targeted system, allowing remote code execution, stealing confidential data, and many more [1]. In total, there are nine types of malware including viruses, RATs, spyware, worms, adware, scareware, bots, ransomware, and cryptominers. Viruses spread harmful code within and between hosts. RATs give attackers remote control. Spyware tracks user activities covertly. Worms replicate and spread through networks. Adware displays unwanted ads. Scareware shows fake alerts to prompt fake antivirus purchases. Bots perform tasks like DDoS attacks. Ransomware encrypts files and demands payment. Cryptominers use resources to mine cryptocurrency [4], [9], [10]. WannaCry, Locky and Jigsaw are examples of ransomware that will be discussed further on.

WannaCry is a well-known ransomware that first appeared in May 2017. This ransomware managed to spread quickly to computers in 150 countries with more than 200,000 infected computers. WannaCry targets computers that use Microsoft Windows as the operating system, encrypts files and then demands a ransom from the attack victims in the form of Bitcoin so that the victims get the decryption key [6]. The WannaCry ransomware was recorded as targeting Windows 7 specifically. WannaCry attacked using a single thread process and then increased the privileges on each document. After that, WannaCry creates a copy of the entire encrypted document and moves it to the %temp% folder with a new file name and extension. WannaCry continued its

attack by using TASKDL.EXE and VSSADMIN.EXE to scramble original files and shadow copy files. In the end, WannaCry changed the desktop wallpaper to threaten victims of the ransomware attack [10].

Another well-known example of ransomware is Locky. Locky first appeared in 2016 by spreading itself through phishing emails. The spread of Locky relies on social engineering techniques to perform tasks that the attacker requires (such as opening infected PDF files). Then Locky will collect information about the environment on the targeted computer. This information is in the form of the language used, IP address, and various existing libraries[11]. Some ransomware encrypts all files found, including the file directory. On the other hand, Locky only encrypts specific document files [14].

Jigsaw is a ransomware variant known for its depiction of characters from the popular film series "Saw" in ransom notes addressed to victims. This ransomware will ask for a ransom of 150 USD or 0.4 Bitcoin. Jigsaw will delete files every hour as long as the victim has not made the ransom. The number of deleted files will continue to increase as long as the ransom is not recovered. If within 72 hours the victim has not paid, Jigsaw will delete all remaining files. If the victim tries to restart their computer, the jigsaw will delete 1000 files every time the computer is restarted [12]. Just like Locky, Jigsaw appeared in 2016 by spreading through phishing emails. Jigsaw is able to encrypt files located on the desktop, documents, pictures, One Drive, Recycle Bin, and C: directory with the exception of files located in protected operating system folders (such as the Program Files folder, Program Files (x86) , and Windows) [6].

### *B. Related Previous Research*

Table I shows related previous research around dynamic analysis on malwares.

TABLE I
RELATED PREVIOUS RESEARCH LITERATURE REVIEW

| Journal | Insight | Method | Contribution |
|---|---|---|---|
| [1] A Comprehensive Review on Malware Detection Approaches (2020) | The paper gives insight about method s and approach on detecting malware, including dynamic analysis. | Signature-based, Behavior-based, Machine Learning based, ynamic Analysis, Static Analysis. | Provides a deep review of the latest malware detection approach and methods used in the approach. |
| [3]A Survey on Malware Analysis Techniques Static, Dynamic, Hybrid, and Memory Analysis (2018) | The paper discusses the techniques for malware analysis. | Static Analysis, Dynamic Analysis, Hybrid Analysis, Memory-based, Feature Extraction, Machine Learning, Forensic Memory Analysis. | Provides a survey towards Malware Analysis Techniques. |
| [4] Dynamic Malware Analysis in the Modern Era—A State of the Art Survey (2019) | The paper discusses the malware detection approach. | Dynamic Analysis, Static Analysis, Hybrid Analysis, Behavior-based Analysis, Machine Learning, Malware Taxonomy, Feature Extraction. | Provides a survey on dynamic malware analysis. Presents three new taxonomy for malware classification based on behavior and access rights. |
| [7] On the classification of Microsoft Windows ransomware using hardware profile (2021) | The paper discusses about how to increase the accuracy of malware detection using hardware-based features. | Hardware-based Feature Approach, Hardware Performance Counter-based Fine-Grained Malware Detection. | Proposes a new malware detection method using dynamic analysis approach. |
| [16]Addressing Crypto-Ransomware Attacks: Before You Decide whether To-Pay or Not-To | The paper discusses about creating a metric to categorize ransomware based on data deletion and file encryption attack structures. | Static Analysis, Dynamic Analysis. | Proposes a new classification algorithm for ransomware categorization. |

## III. RESEARCH METHOD

In this section, we explain the research methodology as depicted in Figure 1. Figure 1 illustrates the system design of our analysis process, beginning with the setup of the analysis environment and culminating in the formulation of conclusions based on our findings.

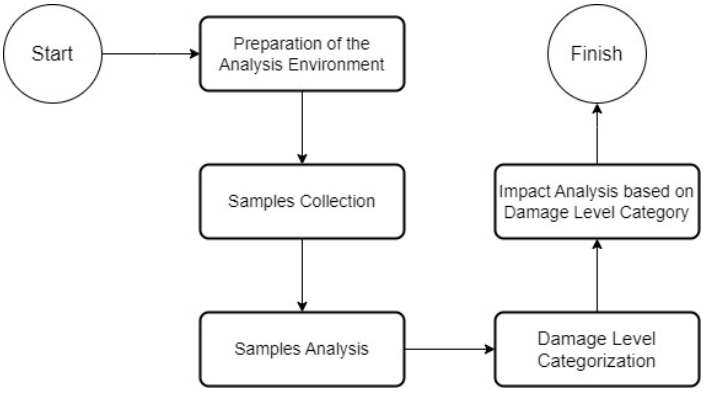


Fig. 1. System Design

### A. *Preparation of the Analysis Environment*

As shown in Figure 2, we utilized VirtualBox to create a virtual machine running the Windows 10 operating system as our analysis environment. To enhance security, we modified the network configuration from NAT to Host-only. This adjustment prevents the samples from requesting network connections from the host machine and mitigates the risk of the ransomware samples escaping the virtual machine.

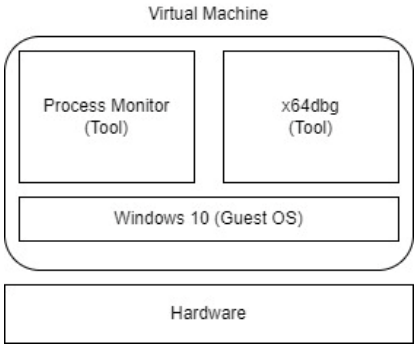


Fig. 2. System Design Specification

Within the virtual machine, we preinstalled the analysis tools Process Monitor and x64dbg. Process monitor is downloaded from Microsoft official website (https://learn.microsoft.com/en-us/sysinternals/downloads/procmon) and x64dbg is downloaded from x64dbg official website (https://x64dbg.com/). This virtual machine setup is primarily used for cloning purposes, ensuring that each ransomware sample is analyzed within its own isolated environment.

### B. *Samples Collection*

Table II categorizes the ransomware samples by family and enumerates the number of samples from each family.

TABLE II
DATASET

| No | Ransomware | Sources | Total of Samples |
|---|---|---|---|
| 1 | WannaCry | https://github.com/kh4sh3i/Ransomware-Samples/tree/main/WannaCry | 1 |
| 2 | Locky | https://github.com/kh4sh3i/Ransomware-Samples/tree/main/Locky | 1 |
| 3 | Jigsaw | https://github.com/kh4sh3i/Ransomware-Samples/tree/main/Jigsaw | 1 |
| **Total of Samples** | | | **3** |

The ransomware samples were sourced from a GitHub repository, where the author has curated a small collection of ransomware organized by family. We downloaded this collection as a protected ZIP file into the virtual machine.

### *C. Samples Analysis*

The analysis was conducted in three virtual machines, each cloned from the initial setup. Each sample was analyzed in its own virtual machine, facilitating the restoration of the virtual machines to their original state by cloning anew as necessary.

During the analysis, we utilized Process Monitor to observe all activities, including file, registry, and network activities. Subsequently, we executed the ransomware samples using x64dbg to maintain control over the running processes. x64dbg also provides information regarding the modules utilized by the ransomware, offering insights into the DLLs employed during execution.

### *D. Damage Level Categorization*

Table III outlines the metrics used in this analysis to categorize the damage level of each ransomware samples [16].

TABLE III
DAMAGE LEVEL CATEGORIZATION

| | Deletion Attack Structure | | | Cryptographic Attack Structure | | | |
|---|---|---|---|---|---|---|---|
| | | | | Single Key Cryptosystem | | Hybrid Key Cryptosystem | |
| **Classification** | **Delete File** | **Overwrite File** | **Delete Volume Shadow Copy** | **Local Key Gen.** | **C2/Embedded** | **Local Key Gen.** | **C2/Embedded** |
| CAT1 | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| CAT2 | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| CAT3 | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| CAT4 | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| CAT5 | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ |
| CAT6 | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| CAT7 | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ |
| CAT8 | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ |

These metrics encompass eight categories of damage levels, ranging from CAT1 (lowest) to CAT8 (highest). The Deletion Attack Structure parameter includes three sub-parameters: Delete File, Overwrite File, and Delete Volume Shadow Copy. The Delete File parameter indicates the ransomware's ability to delete various file types upon execution. The Overwrite File parameter denotes the capability to alter the original content of files, and the Delete Volume Shadow Copy parameter signifies the ability to delete volume shadow copies on Windows 10 [16].

For the Cryptographic Attack Structure, the metrics are divided into two sub-parameters: Single Key Cryptosystem and Hybrid Key Cryptosystem. The Single Key Cryptosystem parameter applies when the ransomware uses either a symmetric or an asymmetric key for encryption and decryption. In contrast, the Hybrid Key Cryptosystem employs both symmetric and asymmetric keys. Both cryptosystem types have additional sub-parameters: Local Key Generation and C2/Embedded. The Local Key Generation parameter indicates that the ransomware generates the key locally on the target machine, while the C2/Embedded parameter signifies key generation under the attacker's instruction via a Command & Control server [16].

### *E. Impact Analysis based on Damage Level Category*

After categorizing all the ransomware samples, the next step involved analyzing the impact of the damage levels. Each category has distinct impacts. For instance, CAT1, also known as the scareware category, lacks encryption and decryption processes and does not delete or overwrite files. In contrast, CAT8 represents the highest damage level, with ransomware samples in this category capable of deleting files, overwriting files, deleting volume shadow copies, and employing a hybrid key cryptosystem generated both locally and through Command & Control instructions [16].

## IV. RESULTS AND DISCUSSION

The results of our analysis were obtained by examining ransomware samples individually and collecting the necessary information to categorize them. Initially, we evaluated the ability of the ransomware samples to delete files, followed by assessments of other parameters. At the end of the analysis, we categorized all three ransomware based on what we have discovered.

### *A. Analyzing Samples for DeleteFile Parameter*

Before executing the ransomware samples with x64dbg, we configured the Process Monitor filter as depicted to monitor the DeleteFile parameter. We utilized SetDispositionInformationFile and SetDispositionInformationEx to track processes that deleted files during the execution of the ransomware samples. This filter configuration was applied to both Jigsaw and Locky, with only the Process Name filter being modified to correspond with the specific sample under analysis. For Jigsaw and Locky, the Process Name filter was renamed to match the currently analyzed sample. After finalizing the filter settings, we applied them and initiated the debugging of the ransomware samples' executable files using x64dbg. WannaCry successfully deleted files, particularly .tmp files. Similarly, Locky and Jigsaw also demonstrated file deletion capabilities when executed with x64dbg.

F Locky had one process that deletes file with the name svchost.exe:Zone.Identifier. Locky also created a subtree named svchost.. Jigsaw employed a subtree as well with the name drpbx.exe to perform deletion processes. Upon completing the DeleteFile parameter analysis, we proceeded to examine the OverwriteFile parameter. For each parameter analysis, we started afresh by cloning the initial virtual machine and deleting previously used virtual machine clones. Table IV summarizes the file types that WannaCry, Locky, and Jigsaw successfully deleted when being executed with x64.dbg.

TABLE IV
DELETED FILE TYPES

| No | Ransomware | File Type |
|---|---|---|
| 1 | WannaCry | .tmp |
| 2 | Locky | .exe:Zone.Identifier |
| 3 | Jigsaw | .dat, .zip, .db, .txt, .xml |

### *B. Analyzing Samples for OverwriteFile Parameter*

In the subsequent analysis step, we modified the Process Monitor filter to display processes that overwrite files.

We applied the same filter settings to both Jigsaw and Locky, with the only variation being the Process Name. After configuring the filters, we applied them and identified processes that overwrote files. Table V shows the file types that WannaCry, Locky, and Jigsaw successfully overwrite when being executed with x64.dbg.

TABLE V
OVERWROTE FILE TYPE

| No | Ransomware | File Type |
|---|---|---|
| 1 | WannaCry | .exe, .pky, .bat, .txt, .png, .svg, .db, .js |
| 2 | Locky | .exe |
| 3 | Jigsaw | .exe, .dat, .zip, .db, .txt, .xml, .ses, .h, .jpg, .js, .svg |

### *C. Analyzing Samples for DeleteVolumeShadowCopy Parameter*

Subsequent to our previous analyses, we evaluated the capability of the ransomware samples to delete volume shadow copies upon execution. Our findings from monitoring activities through Process Monitor indicate that only one of the ransomware samples exhibited the ability to delete volume shadow copies during execution. It is evident that WannaCry utilizes vssadmin, a default Windows utility responsible for managing volume shadow copies. This implies that, upon successful execution of the command, all previously created volume shadow copies are permanently erased, thereby eliminating the possibility of restoring the system via the Windows 10 system recovery feature.

Table VI shows which ransomware samples that is indicated of deleting the volume shadow copy of the virtual machine that they are being executed in.

TABLE VI
DELETION OF VOLUME SHADOW COPY

| No | Ransomware | Volume Shadow Copy Deletion Indication |
|---|---|---|
| 1 | WannaCry | Deletion through running a command with cmd.exe |

### *D. Analyzing Samples for Cryptographic Attack Structure Parameter*

The final step in our analysis of the ransomware samples involves identifying the encryption methods employed by the ransomware. Specifically, we aim to determine whether the ransomware samples utilize symmetric encryption, asymmetric encryption, or a combination of both. Additionally, we investigate whether the encryption keys are generated locally, obtained through a Command & Control (C&C) server, or derived via both methods.

The analysis reveals that WannaCry, Locky, and Jigsaw utilized both AES (symmetric encryption) and RSA (asymmetric encryption) for their encryption processes. Consequently, WannaCry, Locky, and Jigsaw fall into the category of Hybrid Key Cryptosystem. Regarding network activity, our findings indicate that only WannaCry and Locky exhibit network activity upon execution, whereas Jigsaw does not initiate any network processes. This behavior suggests that both WannaCry and Locky may be attempting to communicate with a Command & Control (C&C) server by initiating TCP-related processes. Regarding key generation, our analysis determined that only two out of the three ransomware samples—WannaCry and Jigsaw—performed encryption processes during execution. Conversely, Locky did not engage in file encryption. Instead, Locky masqueraded as svchost.exe and generated TCP requests, seemingly to communicate with the attacker's domain. Due to the absence of an internet connection in the virtual machine environment, Locky was unable to receive encryption-related instructions from the attacker. Consequently, Locky falls under the C2/Embedded sub-parameter. For

WannaCry, the presence of encrypted files even in the absence of an internet connection indicates that WannaCry is capable of generating encryption keys both locally and via a C&C server. Lastly, although Jigsaw did not initiate any TCP-related processes, it was still able to encrypt files, indicating that Jigsaw generates encryption keys locally.

Table VII shows the cryptographic attack structure of all ransomware samples including the network activities.

TABLE VII
CRYPTOGRAPHY STRUCTURE AND NETWORK ACTIVITY

| No | Ransomware | Cryptography Attack Structure | Network Activities |
|---|---|---|---|
| 1 | WannaCry | Uses both AES and RSA encryption. | Found |
| 2 | Locky | Uses both AES and RSA encryption | Found |
| 3 | Jigsaw | Uses both AES and RSA encryption | Not found |

### *E. Categorizing the Ransomware Samples*

With the necessary data collected to categorize the damage levels of WannaCry, Locky, and Jigsaw, we can now apply our established metrics to each ransomware samples as shown in Table VIII.

TABLE VIII
RANSOMWARE SAMPLES CATEGORIZATION

| | Deletion Attack Structure | | | Cryptographic Attack Structure | | | |
|---|---|---|---|---|---|---|---|
| | | | | Single Key Cryptosystem | | Hybrid Key Cryptosystem | |
| Ransomware | Delete File | Overwrite File | Delete Volume Shadow Copy | Local Key Gen. | C2/Embedded | Local Key Gen. | C2/Embedded |
| Jigsaw | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| Locky | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ |
| WannaCry | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ |

Based on the data obtained from our analysis, it is evident that the WannaCry ransomware sample possesses the capability to delete files, overwrite files, and delete volume shadow copies. Regarding its cryptographic attack structure, WannaCry is capable of generating encryption keys both locally and via a Command & Control (C&C) server. This conclusion is supported by our findings, which indicate that WannaCry was able to encrypt files in a virtual machine without network connectivity while also attempting to connect to the attacker's C&C server.

In the case of Locky, the ransomware sample demonstrated the ability to delete files, overwrite files, and generate encryption keys through the attacker's C&C server. Our findings indicate that Locky did not encrypt any files within the virtual machine; instead, it disguised itself as svchost.exe and attempted network connections to the attacker's C&C server.

Conversely, Jigsaw exhibited the capability to delete files, overwrite files, and generate encryption keys locally, as our analysis revealed that Jigsaw did not attempt any network connections during execution but still able to encrypt files within the virtual machine.

For the cryptosystem, all three ransomware samples—WannaCry, Locky, and Jigsaw—employ the symmetric key AES and the asymmetric key RSA for their encryption processes. To address the missing proof for the Delete Volume Shadow Copy parameter of Locky and Jigsaw, we referenced a similar study conducted by Chisimba et al. (2019), which reported that both Locky and Jigsaw were capable of deleting volume shadow copies created by Windows XP, Windows Vista, Windows 7, and Windows 10 [16]. Having successfully

addressed all parameters, we can now classify the ransomware samples as follows: Jigsaw is categorized as CAT6 ransomware, Locky is categorized as CAT7 ransomware, and WannaCry is categorized as CAT8 ransomware.

### *F. Impact Analysis based on Damage Level Category*

Currently, we have classified Jigsaw, Locky, and WannaCry as CAT6, CAT7, and CAT8 ransomware, respectively. The subsequent phase of this research involves analyzing the impacts of each ransomware sample's damage level category on the victims of the ransomware attacks.

According to the damage level categorization framework, it is possible for victims to recover data affected by both the deletion and cryptographic attacks of a ransomware incident. Data lost due to the deletion attack structure can potentially be retrieved using third-party recovery tools. However, recovering data compromised by a cryptographic attack typically requires obtaining the decryption key. This can be achieved either by paying the ransom or by exploiting the decryption key generation that occurs on the host machine. Recovery is feasible for ransomware that generates encryption keys locally rather than via the attacker's Command & Control (C&C) instructions. Consequently, it is possible to recover the decryption keys for Jigsaw and WannaCry, as both ransomware samples were able to encrypt files without network connectivity. In contrast, recovery is impossible for Locky, as it does not generate encryption keys locally.

## V. CONCLUSION

From the results of our analysis using tools such as Process Monitor and x64dbg, along with the categorization framework for ransomware attack damage levels, we have derived several key insights. The use of Process Monitor and x64dbg significantly enhances our understanding of ransomware behavior by providing deep insights into system activities during infection. These tools enable us to track the interactions of ransomware with the operating system, registry, and other processes.

The categorization framework we employed allows us to classify the damage levels of ransomware attacks based on both deletion attack structures and cryptographic attack structures. This framework facilitates a detailed understanding of the behavioral patterns and impacts of ransomware. Our analysis identified the damage levels of attacks from three ransomware samples: CAT8 for WannaCry, CAT7 for Locky, and CAT6 for Jigsaw. These ransomware attacks involve file deletion, file overwriting, volume shadow copy deletion, file encryption, local key generation, and potential communication with Command and Control (C2) servers.

Dynamic analysis for damage level categorization of ransomware attacks using this framework, with the aid of Process Monitor and x64dbg, has proven to be effective enough to yield accurate results with low resource requirements. However, it is important to note that Process Monitor and x64dbg were unable to detect the deletion of volume shadow copies for two out of the three ransomware samples. Future work should focus on developing new tools and methods such as using both static and dynamic analysis approach to more effectively track volume shadow copy deletion. We believe that the dynamic analysis approach, using the framework we applied, demonstrates significant effectiveness in categorizing the damage levels of ransomware attacks and analyzing the impacts of the attacks.

## DATA AND COMPUTER PROGRAM AVAILABILITY

Data and program used in this paper can be accessed in the following site:
https://github.com/kh4sh3i/Ransomware-Samples.

## REFERENCES

[1] O. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," *IEEE Access*, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 6249–6271, 2020. doi: 10.1109/ACCESS.2019.2963724.

[2] A. Afianian, S. Niksefat, B. Sadeghiyan, and D. Baptiste, "Malware dynamic analysis evasion techniques: A survey," *ACM Comput Surv*, vol. 52, no. 6, Nov. 2019, doi: 10.1145/3365001.

[3] R. Sihwail, K. Omar, and K. A. Z. Ariffin, "A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis," *International Journal on Advanced Science Engineering and Information Technology*, vol. 8, pp. 4–6, 2018.

[4] O. Or-Meir, N. Nissim, Y. Elovici, and L. Rokach, "Dynamic malware analysis in the modern era—A state of the art survey," *ACM Comput Surv*, vol. 52, no. 5, Sep. 2019, doi: 10.1145/3329786.

[5] H. Zhao, M. Li, T. Wu, and F. Yang, "Evaluation of Supervised Machine Learning Techniques for Dynamic Malware Detection," *International Journal of Computational Intelligence Systems*, vol. 11, pp. 1153 – 1169, 2018.

[6] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Comput Secur*, vol. 111, Dec. 2021, doi: 10.1016/j.cose.2021.102490.

[7] S. Aurangzeb, R. N. Bin Rais, M. Aleem, M. A. Islam, and M. A. Iqbal, "On the classification of Microsoft-Windows ransomware using hardware profile," *PeerJ Comput Sci*, vol. 7, pp. 1–24, 2021, doi: 10.7717/peerj-cs.361.

[8] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms," *Journal of Telecommunications and Information Technology*, no. 1, pp. 113–124, 2019, doi: 10.26636/jtit.2019.130218.

[9] L. Y. Connolly, D. S. Wall, M. Lang, and B. Oddson, "An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability," *J Cybersecur*, vol. 6, no. 1, 2020, doi: 10.1093/CYBSEC/TYAA023.

[10] T. R. Reshmi, "Information security breaches due to ransomware attacks - a systematic literature review," *International Journal of Information Management Data Insights*, vol. 1, no. 2. Elsevier Ltd, Nov. 01, 2021. doi: 10.1016/j.jjimei.2021.100013.

[11] R. Moussaileb, N. Cuppens, J. L. Lanet, and H. Le Bouder, "A Survey on Windows-based Ransomware Taxonomy and Detection Mechanisms: Case Closed?," *ACM Computing Surveys*, vol. 54, no. 6. Association for Computing Machinery, Jul. 01, 2021. doi: 10.1145/3453153.

[12] G. McDonald, P. Papadopoulos, N. Pitropakis, J. Ahmad, and W. J. Buchanan, "Ransomware: Analysing the Impact on Windows Active Directory Domain Services," *Sensors*, vol. 22, no. 3, Feb. 2022, doi: 10.3390/s22030953.

[13] I. Kara and M. Aydos, "The rise of ransomware: Forensic analysis for windows based ransomware attacks," *Expert Syst Appl*, vol. 190, Mar. 2022, doi: 10.1016/j.eswa.2021.116198.

[14] B. Yamany, M. S. Elsayed, A. D. Jurcut, N. Abdelbaki, and M. A. Azer, "A New Scheme for Ransomware Classification and Clustering Using Static Features," *Electronics (Switzerland)*, vol. 11, no. 20, Oct. 2022, doi: 10.3390/electronics11203307.

[15] J. H. Park, S. K. Singh, M. M. Salim, A. E. L. Azzaoui, and J. H. Park, "Ransomware-based Cyber Attacks: A Comprehensive Survey," *Journal of Internet Technology*, vol. 23, no. 7, pp. 1557–1564, 2022, doi: 10.53106/160792642022122307010.

[16] A. Zimba, Z. Wang, and M. Chishimba, "Addressing Crypto-Ransomware Attacks: Before You Decide whether To-Pay or Not-To," *Journal of Computer Information Systems*, vol. 61, no. 1, pp. 53–63, 2021, doi: 10.1080/08874417.2018.1564633.