JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2056-2068

DYNAMIC ANALYSIS OF RANSOMWARE BEHAVIOR ON WINDOWS OPERATING SYSTEM

Addin Amanatulloh Suparjo[1)], Muhamad Irsan*[2)], Erwid Mustofa Jadied[3)]
1. Faculty of Informatics, Telkom University, Bandung, Indonesia
2. Faculty of Informatics, Telkom University, Bandung, Indonesia
3. Faculty of Informatics, Telkom University, Bandung, Indonesia

Article Info
Keywords: Behavior; Cybersecurity; Detection System; Dynamic Analysis; Ransomware

Article history:
Received 19 Agustus 2024
Revised 30 September 2024
Accepted 5 Oktober 2024
Available online 1 September 2025

DOI :
https://doi.org/10.29100/jipi.v10i3.6381

*Corresponding author.
Muhamad Irsan
E-mail address:
irsanfaiz@telkomuniversity.ac.id

ABSTRACT
Ransomware is a type of malicious software capable of disabling computer functions or encrypting all files, resulting in significant disruption. This research dynamically analyzes ransomware behavior on the Windows 11 operating system. Several ransomware samples were executed and analyzed to obtain a list of ransomware behaviors used for performance testing on the samples. This topic is important as ransomware attacks have increased significantly and become one of the most destructive cyber threats. Ransomware attacks have caused major disruptions to services such as BSI banking, making it crucial in this digital era to understand the behavior of suspicious files or processes and how to mitigate such threats.
This study conducts dynamic analysis of ransomware behavior on the Windows 11 operating system. In an isolated environment using Virtual Machines (VMs), this research employs tools such as Process Monitor, Wireshark, and ProcDOT to collect data and visualize ransomware behavior. The results of this study include the compilation of a list of ransomware behaviors used to build a detection system that can identify samples based on detected behaviors. The developed detection system shows a good detection rate, which has a detection percentage of 69%. These results show significant potential in identifying ransomware threats, although there is still space for improvement and further development.

.

I. INTRODUCTION

RANSOMWARE is a type of malicious software and one of the types of malware that, when activated, will disable computer functions or encrypt all files within it [1]. Ransomware can do this in various ways, such as locking the infected computer's desktop or encrypting all its files. Additionally, ransomware can be used to steal money or damage critical infrastructure by encrypting files and data on the target computer [2]. Unlike other types of cyber-attacks that might leave some parts of the system functional, ransomware attacks pose a serious security threat as they can halt key operations within a business system. The shift in focus from individuals to businesses and organizations is primarily driven by the potential for greater profit [3].

The topic of ransomware behavior analysis is very interesting and relevant in today's cybersecurity landscape. Ransomware attacks have increased significantly in recent years, becoming one of the most destructive and damaging cyber threats to many organizations and individuals. In the current digital era, it is crucial to maintain data and information security and understand how to tackle such threats [1] [4]. Previous ransomware research has mostly focused on static analysis, which does not reflect the actual behavior of ransomware when executed. This study focuses on dynamic analysis methods, allowing for direct observation of how ransomware spreads, encrypts files, and other malicious behaviors [5].

This research focuses on the details of ransomware attacks on the Windows 11 operating system, considering the significant impact and economic losses caused to both individuals and organizations. Most previous research has used older versions of Windows, such as Windows 7 or Windows 10, so this research will provide new insights into how ransomware operates on Windows 11 with its more advanced security features [6]. The research will be conducted by running ransomware samples on Windows 11 installed on a VirtualBox. The ransomware samples include Cerber, Locky, WannaCry, and Mamba. Subsequently, the analysis phase will use tools such as Procmon (Process Monitor), Wireshark, and ProcDOT. Procmon records system activity in real-time, including running processes, file operations, registry activities, and network activities [7]. Wireshark captures and analyzes network traffic, including data packets sent and received over the network [8]. ProcDOT takes data from Procmon and

Wireshark to provide an easily understandable visualization of how malware interacts with the system [9]. The integration of these analysis tools will provide a more comprehensive idea of ransomware behavior [10].

A ransomware incident occurred in Indonesia in May 2023, when PT. Bank Syariah Indonesia Tbk (BSI) experienced a disruption in its digital services, allegedly due to a LockBit 3.0 ransomware attack. The attack caused prolonged service disruptions, preventing customers from conducting transactions or receiving banking services. The hacker group posing as LockBit claimed responsibility and threatened to release the personal information of BSI customers and employees unless a ransom was paid [11].

The objectives of this research are to analyze the behavior of ransomware in an isolated Windows 11 environment, with the results of this analysis being a list of ransomware behaviors used to build a performance testing system. The second objective is to analyze the performance in detecting ransomware using the detection system built in the previous stage.

Ransomware research has become an important topic, with various studies being conducted to understand how ransomware attacks work and reduce their impact. There is research analyzing ransomware behavior at scale, using over 1.7 billion lines of I/O request packets (IRPs) and file system event logs. The findings showed that ransomware tends to access non-system files, perform aggressive file system activity, and modify various file types with high frequency. The strengths of the study are the large scale of analysis and behavior-based approach, which provide deep insights for developing more effective ransomware detection and prevention solutions. However, the limitations of this research are the data that may not represent all ransomware variants and the lack of focus on practical implementation [9].

There are also other studies that propose ransomware detection systems based on dynamic API calls (CFG) and data mining techniques such as Random Forest (RF), Support Vector Machine (SVM), Simple Logistic (SL), and Naive Bayes (NB). The findings show that this approach is more effective in detecting ransomware that uses obfuscation and polymorphism techniques. The strengths of this research include an increase in detection accuracy of up to 98.2% with the Simple Logistic algorithm. However, limitations include limited datasets and implementation complexity that requires high computational resources [10].

This research is hoped to make a significant contribution to the field of cybersecurity, especially in terms of understanding and addressing ransomware threats in the Windows 11 environment. By dynamically analyzing ransomware behavior, this research offers deep insight into how ransomware exploits or adapts to the latest security features in Windows 11 [12]. In addition, the integration of data from tools such as Procmon, Wireshark, and ProcDOT enables the development of more comprehensive ransomware detection patterns, which can be used to create more accurate and responsive detection systems [13]. The methodology applied in this research also has the potential to become a new framework in ransomware analysis, potentially allowing other researchers to analyze different types of ransomwares with a more comprehensive approach [14].

The results of this study can also be used by organizations to strengthen their cybersecurity policies, reduce the risk and impact of ransomware attacks, and protect sensitive data. This research also adds insight into how network traffic generated by ransomware can be analyzed for early detection, which is important for strengthening network security infrastructure [15]. The research should consequently enrich the cybersecurity literature with new empirical data relevant for modern environments, helping to update and reinforce the knowledge base in this field [16].

II. Research Methodology

Figure 1 is the research framework used to analyze ransomware behavior on the Windows 11 operating system dynamically. This system is designed to create a secure testing environment and enable direct observation of ransomware behavior.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2056-2068

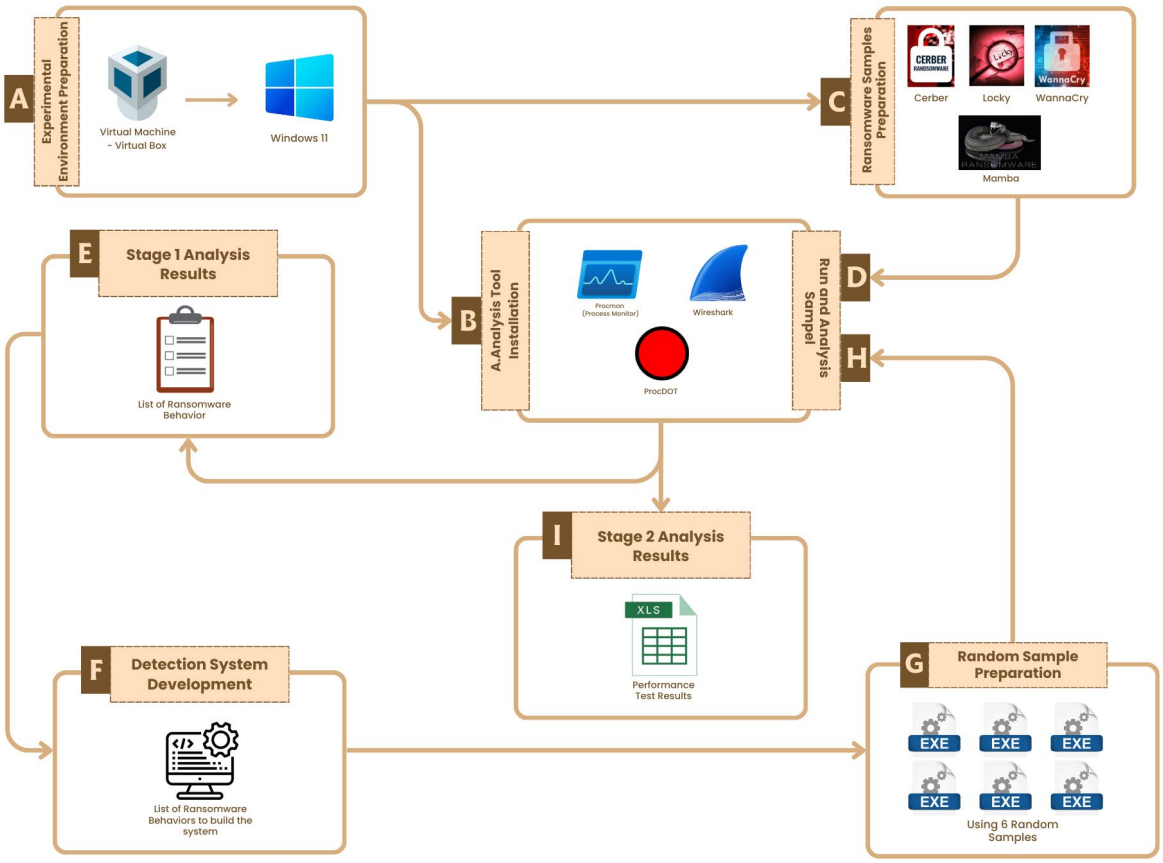

Fig. 1. Research Framework

A. *Experimental Environment Preparation*

Table I describes the hardware specifications used in this research.

TABLE I
HARDWARE SPECIFICATIONS

Hardware	Information
Processor	11th Gen Intel(R) Core (TM) i7-11370H @ 3.30GHz (8 CPUs), ~3.3GHz
Memory	24GB (24576MB RAM)
SSD	464.3 GB
Operating System	Windows 11 Home Single Language 64-bit (10.0, Build 22631)

Table II describes the software specifications used in this research.

TABLE II
SOFTWARE SPECIFICATIONS

Software	Functions
Oracle VM VirtualBox 7.0.18	As an isolated virtual environment and used to independently install the Windows 11 operating system.
Windows 11 Pro 64-bit	As the main operating system in VirtualBox, it was used to run the samples used in the study. Later, Windows 11 will be snapshot from before to after conducting analysis experiments. The function of the snapshot is to restore the VM or windows 11 to the initial condition before conducting the analysis experiment.

To ensure the security of the test environment and prevent the analyzed ransomware from spreading to other systems, several important steps were implemented. The analysis is performed in a virtual machine (VM) that is completely isolated from the network and other devices. These virtual machines were created using a hypervisor such as VirtualBox and snapshots were taken before running the ransomware to allow a restore to the previous system in the event of a breakdown. Furthermore, the network connection on the virtual machine uses a strict firewall to restrict the ransomware's access.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2056-2068

B. *Analysis Tool Installation*

The analysis in this study uses three tools that will be installed on the Windows 11 operating system. These tools are Procmon (Process Monitor), Wireshark, and ProcDOT. The analytical tools used and functions can refer to table III.

TABLE IIII
ANALYSIS TOOL SPECIFICATIONS

Analysis Tool	Functions
Process Monitor v4.01	Procmon is useful for analyzing software behavior, detecting suspicious activity, and troubleshooting system performance issues.
Wireshark 4.2.6	Wireshark captures and analyzes network traffic, and includes data packets sent and received over the network.
ProcDOT 1.22	ProcDOT takes data from Procmon and Wireshark to provide an easy-to-understand visualization of how malware interacts with the system.

Procmon (Process Monitor), Wireshark, and ProcDOT were chosen based on the need to monitor system activity in depth, analyze network traffic, and combine information in an easily accessible visual form [17]. Other tools such as Cuckoo Sandbox were considered, but not chosen due to the inadequate computer specifications used in this study. Cuckoo Sandbox requires higher computer specifications, especially when analyzing many samples or performing repeated analysis [18].

There are also other tools such as Sysmon, Tcpdump, and Volatility that were also considered. Sysmon allows detailed monitoring of system activity but requires complex configuration [19]. Tcpdump is a powerful tool for capturing packets but lacks in providing an easy-to-understand user interface [20]. Volatility is used for memory analysis but does not offer the same integration as the other selected tools [21]. Therefore, these tools were not selected as they did not offer the same combination of flexibility, ease of use, and integration as the selected tools.

C. *Ransomware Samples Preparation*

This section is a sample collection to perform stage 1 analysis. The analysis uses 4 samples that indicate ransomware. Table IV details the sampling used and its sources.

TABLE IV
RANSOMWARE SAMPLES FOR STAGE 1 ANALYSIS

No	Ransomware Family	Source	Years
1	Cerber	https://github.com/kh4sh3i/Ransomware-Samples	2021
2	Locky	https://github.com/kh4sh3i/Ransomware-Samples	2021
3	WannaCry	https://github.com/kh4sh3i/Ransomware-Samples	2021
4	Mamba	https://github.com/kh4sh3i/Ransomware-Samples	2021

The ransomware samples used in this study were taken from the GitHub repository “Ransomware-Samples by kh4sh3i”. Each sample was compressed with a password to prevent accidental execution during extraction.

To ensure the validity and representativeness of the samples, each sample was verified using a hash (such as SHA-256) to ensure there were no modifications and show that the sample corresponds to a ransomware version recognized by the cybersecurity community. After verification, the samples were run in the secure virtual environment of VirtualBox to ensure that they show typical ransomware behavior, such as file encryption or desktop locking. The samples also include a variety of ransomware types that represent recent attack trends, so that the analysis can provide a representative picture of the ransomware threat on modern operating systems such as Windows 11 [22].

D. *Run and Analysis Sampel*

After collecting samples that indicate ransomware, the samples will then be analyzed. Figure 2 is a flowchart of the analysis steps using this tool.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2056-2068

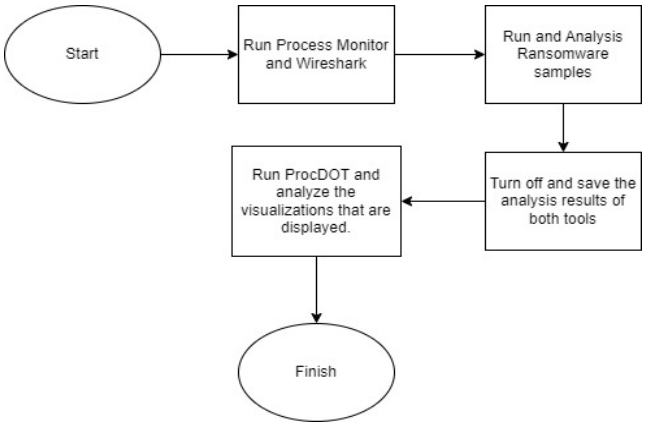

Fig. 2. Flowchart of Analysis Steps Using the Tools

1) Run Process Monitor and Wireshark

Run the Process Monitor analysis tool and turn off the "Show Resolve Network Addresses" feature and set the columns you want to display. Figure 3 is an example of feature settings in Process Monitor.

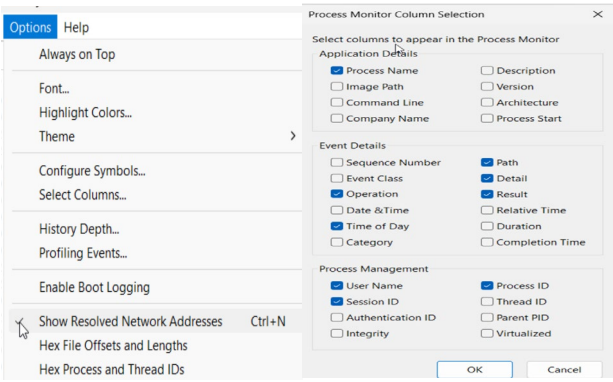

Fig. 2. Process Monitor Setting

After running Process Monitor, also run Wireshark and select the network interface being used. Press "Start Capturing Packets" to start the analysis.

2) Run and Analysis Ransomware samples

After running both tools, run the ransomware sample. If the sample file format is other than .exe, it must first be converted to that file format. After that, it is run and analyzed for 5-10 minutes. The analysis duration was chosen based on some practical considerations in ransomware studies. This duration is sufficient to observe the initial phases of ransomware activity, including the encryption process, communication with the command-and-control (C2) server, and modification of systems such as the registry or files. Ransomware typically performs these actions early on after execution to maximize its impact before it is detected or stopped. A short analysis duration may not be enough to capture all ransomware behaviors, especially if the ransomware has execution delay mechanisms or activities triggered by certain conditions, such as system reboots. While a duration of 5-10 minutes can provide an overview, a longer analysis or under different conditions may be required to ensure all aspects of ransomware behavior are identified.

3) Turn off and save the analysis results of both tools

After analyzing for 5-10 minutes, turn off or stop the process of both tools and save the analysis results. For Process Monitor the analysis result file is saved in .CSV format while Wireshark is saved in .txt or .pcap format. Figure 4 is a view of the file format used to save the analysis results.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2056-2068

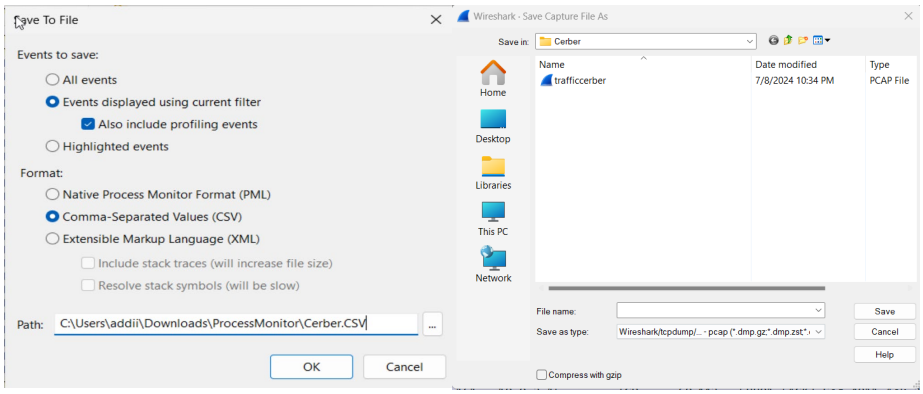

Fig. 3. Process Monitor and Wireshark Format File

4) Run ProcDOT and analyze the visualizations that are displayed.

After analyzing with Process Monitor and Wireshark, proceed to run ProcDOT and insert the analysis files from these two tools. Then, select the launcher that matches the sample being analyzed. After that, refresh, and ProcDOT will produce a visualization of the analysis results using Process Monitor and Wireshark. Figure 5 is the visualization view in ProcDOT.

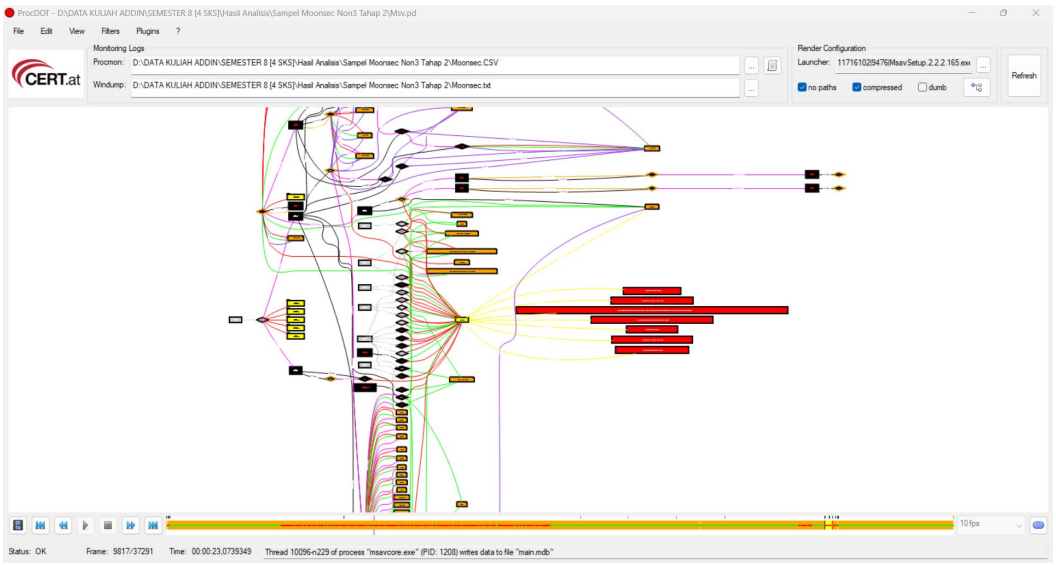

Fig. 4. ProcDOT Display

E. Stage 1 Analysis Results

After analyzing the visualization using ProcDOT, the result of stage 1 analysis is a list of behaviors from each ransomware sample. The behavior list will be used for the next stage of analysis.

F. Detection System Development

After receiving a list of behaviors from each analyzed ransomware sample, this list is summarized and used to develop a working detection system for performance testing. The detection system will determine whether a random sample tested in stage 2 is ransomware or not.

G. Random Sample Preparation

This section is the collection of samples to perform stage 2 analysis. This analysis used 6 random samples from various sources. Table V shows the samples used and their sources.

TABLE V
RANDOM SAMPLES FOR STAGE 2 ANALYSIS

No	Sampel Name	Source	Type File	Years
1	Unamed	https://github.com/kh4sh3i/Ransomware-Samples	Ransomware	2021
2	Matsnu	https://github.com/kh4sh3i/Ransomware-Samples	Ransomware	2021
3	Simutrans Simulator	https://sourceforge.net/projects/simutrans/	Games	2024

4	Wesnoth	https://sourceforge.net/projects/wesnoth/	Games	2024
5	Moon Secure Antivirus	https://sourceforge.net/projects/moonav/	Antivirus	2022
6	AnyDesk	https://anydesk.com/en/downloads/windows	Remote Dekstop	2024

H. Run and Analyze Sampel

In this stage 2 analysis, the tools and analysis steps used are the same as in stage 1 analysis. The difference is only the sample used.

I. Stage 2 Analysis Results

The result of stage 2 analysis is a detection system that has a percentage value as its reference. The system will determine whether the analyzed sample is ransomware or not based on a list of existing behaviors.

III. Result and Discussion

A. Testing Results

1) Stage 1 Testing Results

In this first stage of analysis, a list of ransomware behaviors was collected from analyzing 4 samples indicated by ransomware. The following is the list of behaviors obtained.

a. Samplel Locky

- Creates a new registry key value
- Changes registry values with specific parameters or configurational values.
- Creates a new temporary file
- Renames a file using a thread that runs during monitoring and stops when monitoring is complete
- Deletes a file using a thread that runs during monitoring and stops when monitoring is complete
- Creates a permanent new file
- Locky.exe file deleted by threads (6324) that were run during monitoring and stopped when monitoring was complete
- Svchost.exe deleted by threads (6324) that were run during monitoring and stopped when monitoring was complete
- Created new threads during monitoring to help create new files and stopped when monitoring was complete
- Read the files in the Detection History folder

b. Sample Cerber

- Changing the desktop wallpaper
- Using windows utilities (cmd.exe and mshta.exe) to execute malicious commands
- Making modifications to the registry
- Renaming files deleted during monitoring
- Renaming files that still exist after monitoring
- Encrypting files (documents, photos, and databases)
- Writing History.Log files
- Creates a thread during monitoring and is terminated after monitoring is complete
- Created new files (_R_E_A_D___T_H_I_S___APWG_.txt and _R_E_A_D___T_H_I_S___APWG_.hta) that contain links used for users to pay a ransom in order to get the file description key and can only be accessed for a limited time.
- Deploy the new file to each folder
- Communicate with the external server (C2) using UDP.

c. Sample WannaCry

- Using threads to create new files with .wnry format
- WannaCry.exe file deleted by threads (11184) that were run during monitoring
- Renamed files that were still present after monitoring
- Creates a new file that still exists after monitoring
- Created a new process that was created during monitoring and stopped at the end of monitoring
- Process WannaCry.exe (PID: 8312) deleted/Kill Own Process by thread (6296)

- Registry modification (set as value) involving windows tools (icacls.exe and attrib.exe).
- Write and read History.Log file
- Writing Detection.Log file

d. *Sample Mamba*
- The 131.exe file loads threads (2212 and 5076), after which the two threads delete the 2 processes created during monitoring (131.exe PID: 6440 and 131.exe PID: 9424).
- Created process during monitoring and terminated after monitoring was completed
- Renamed a file during monitoring
- Created a new file that still exists after monitoring is complete
- Modify registry values in cmdrun.exe and cache_dataf files
- Read suspected Windows Defender work, maintenance, clean up, schedule scan, and verification schedules to manipulate these tasks to hide their activity or run malware at certain times.
- Writes History.Log file
- Writing Detection.Log file

After preparing a list of behaviors from 4 samples that indicated ransomware, the list of behaviors was summarized into 20 behaviors used to build the detection system. The following is the list of behaviors used to build the detection system categorized by encryption, persistence, deployment and management, self-destruction, operation, external communication, and utilities and tools.

a. *Encryption*
- Encrypt a file\

b. *Persistence*
- Modify registry values
- Create a new process that is permanent
- Create a new file that is permanent

c. *Deployment and Management*
- Delete an existing file
- Rename existing files or new files
- Create new files that are temporary or temporary
- Create a new process that is temporary or temporary
- Create a new thread that is permanent
- Create a new thread that is temporary or temporary
- Using a thread that is permanent
- Using a thread that is temporary or temporary

d. *Self-destruction*
- Kill own process or delete own process

e. *Operations*
- Change wallpaper or desktop display
- Write .Log files
- Read available files
- Creating a new file format

f. *External Communication*
- Communicate with an external server (C2)
- Send a message containing a link for ransom payment

g. *Utilities and Tools*
- Using windows tools or utilities

Figure 6 is a diagram of the distribution of ransomware behavior by category. The behavior category Deployment and management produced the most results in the analysis.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2056-2068

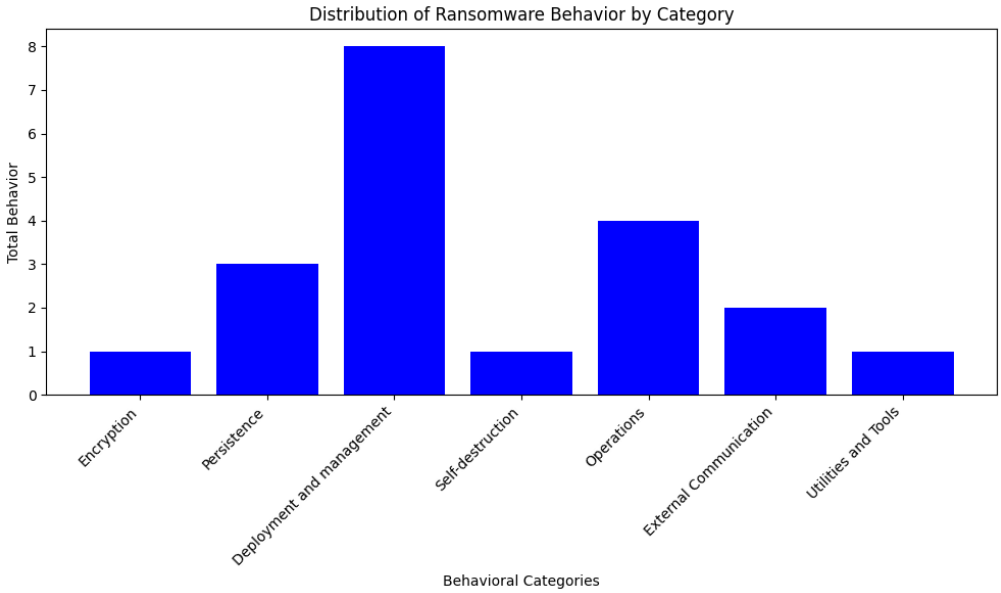

Fig. 5. Distribution of Ransomware Behavior by Category

2) Stage 2 Testing Results

In the second stage of analysis, the summarized behavior list is used to build a sample detection system or performance test. The performance test uses 6 samples (2 samples indicated by ransomware and 4 samples not indicated by ransomware). The following are tables VI, VII, and VIII which show the results of the performance test analysis using the detection system that has been developed.

TABLE VI
UNAMED AND MATSNU DETECTION SYSTEM

Behavior List	Unamed	Matsnu
Change the wallpaper or desktop display	0	0
Kill own process or delete own process	1	1
Delete available files	1	1
Encrypt a file	1	1
Modify registry values	1	1
Rename existing or new files	1	1
Create a new process that is permanent	1	0
Create a new process that is temporary or temporary	1	1
Create a new file that is permanent	1	1
Create a new file that is temporary	1	1
Create a new thread that is permanent	1	0
Create a new thread that is temporary	1	0
Using a thread that is permanent	1	1
Using a thread that is temporary	1	1
Writing a .Log file	1	1
Communicate with an external server (C2)	0	1
Read available files	1	1
Creating a new file format	0	0
Using windows tools or utilities	0	1
Sending a message with a link for ransom payment	0	0
TOTAL	15	14
TOTAL SCORE	20	20
Percentage	75%	70%
System Detection (Declared Ransomware If Percentage > 69%)	Ransomware	Ransomware
ACTUAL VALUE	Ransomware	Ransomware

TABLE VII
SIMUTRANS SIMULATOR AND WESNOTH DETECTION SYSTEM

Behavior List	Simutrans Simulator	Wesnoth
Change the wallpaper or desktop display	0	0
Kill own process or delete own process	1	1
Delete available files	0	0
Encrypt a file	0	0
Modify registry values	1	1
Rename existing or new files	0	1
Create a new process that is permanent	0	0

Create a new process that is temporary or temporary	1	1
Create a new file that is permanent	1	1
Create a new file that is temporary	0	1
Create a new thread that is permanent	0	0
Create a new thread that is temporary	0	1
Using a thread that is permanent	1	1
Using a thread that is temporary	1	1
Writing a .Log file	0	1
Communicate with an external server (C2)	1	0
Read available files	1	1
Creating a new file format	0	0
Using windows tools or utilities	0	0
Sending a message with a link for ransom payment	0	0
TOTAL	8	11
TOTAL SCORE	20	20
Percentage	40%	55%
System Detection (Declared Ransomware If Percentage > 69%)	Not Ransomware	Not Ransomware
ACTUAL VALUE	Not Ransomware	Not Ransomware

TABLE VIII
MOON SECURE ANTIVIRUS AND ANYDESK DETECTION SYSTEM

Behavior List	Moon Secure Antivirus	AnyDesk
Change the wallpaper or desktop display	0	0
Kill own process or delete own process	0	0
Delete available files	0	0
Encrypt a file	0	0
Modify registry values	1	1
Rename existing or new files	0	1
Create a new process that is permanent	1	1
Create a new process that is temporary or temporary	1	1
Create a new file that is permanent	1	1
Create a new file that is temporary	0	1
Create a new thread that is permanent	1	1
Create a new thread that is temporary	1	1
Using a thread that is permanent	1	1
Using a thread that is temporary	1	0
Writing a .Log file	1	1
Communicate with an external server (C2)	0	1
Read available files	1	1
Creating a new file format	0	0
Using windows tools or utilities	1	1
Sending a message with a link for ransom payment	0	0
TOTAL	11	13
TOTAL SCORE	20	20
Percentage	55%	65%
System Detection (Declared Ransomware If Percentage > 69%)	Not Ransomware	Not Ransomware
ACTUAL VALUE	Not Ransomware	Not Ransomware

B. *Analysis of Testing Results*

1) *Analysis of Stage 1 Testing Results*

Based on the test results of four samples that indicated ransomware, a list of 20 ransomware behaviors that have been split into 7 categories has been obtained. This list of behaviors is used to build a detection system at a subsequent stage. The behaviors used to build the detection system are behaviors that are often present in samples that are indicated by ransomware analyzed using the ProcDOT tool.

2) *Analysis of Stage 2 Testing Results*

Based on the results of the detection system testing that has been carried out, a sample is declared as ransomware-ware if the detection percentage value is more than 69%. The threshold is used based on the lowest detection percentage in the sample indicated by ransomware, namely Matsnu.exe, which has a detection percentage of 70%. Therefore, a threshold of 69% was chosen to ensure that all ransomware samples were effectively detected, including those with the lowest detection percentage values. And also the threshold was used because after calculating using confusion matrix, the threshold resulted in accuracy, precision, recall, and F1-Score of 100%.

Before setting the 69% threshold, testing was done with several other thresholds, namely 50%, 60%, 70%, and 80%. The calculation also uses confusion matrix and based on the analysis of test results with various thresholds, the 69% threshold provides the most optimal detection results, with the minimum false positive and false

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2056-2068

negative rates. And the determination of this threshold is subjective. Figure 7 is a visualization of Accuracy, Precision, Recall, and F1-Score at different thresholds.

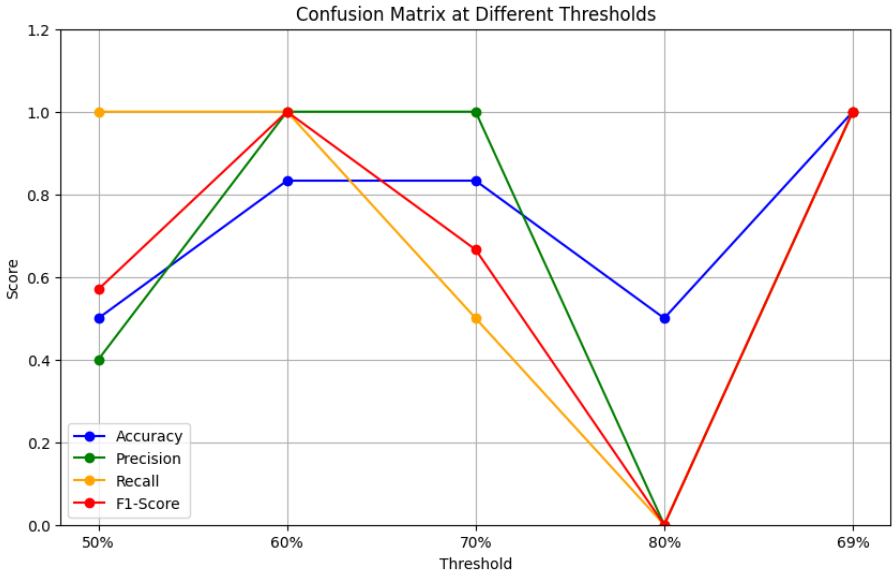

Fig. 6. Confusion Matrix at Different Thresholds

C. *Implications and Constraints*

The research results on ransomware detection systems have significant practical implications in protecting organizations from ransomware attacks. These systems can recognize early indications of ransomware activity, such as data encryption or file name changes, thus enabling security teams to take preventive action before the attack fully takes place. With a faster response, organizations can isolate infected devices and limit the spread of ransomware. The data collected from these systems can also be used to strengthen security policies by identifying weak points in the infrastructure. Overall, these detection systems are important for improving an organization's resilience to cyber threats.

However, there are some constraints to consider. One is the limited ransomware sample, which may not cover all ransomware types and variants, reducing the system's ability to detect new threats. Also, the analysis methods used can be too specific, making the system less adaptive to more sophisticated ransomware techniques.

Previous related research has introduced Unveil, a framework that detects ransomware through dynamic analysis by monitoring system file changes and encryption activity. That approach is effective for various ransomware families but focuses on changes that occur after the ransomware is active [23]. In comparison, this research focuses on identifying ransomware behavior before encryption is performed, by utilizing a list of behaviors specifically designed to detect suspicious actions in the early stages of an attack. This allows for a faster response before significant damage is done.

IV. CONCLUSION

Based on the results of research on dynamic analysis of ransomware behavior on Windows 11 operating systems, the conclusion can be obtained that a ransomware detection system was successfully created using a list of behaviors identified from the analyzed ransomware samples. A detection threshold of 69% was chosen based on the Matsnu.exe sample, which had the lowest detection percentage of 70%. This threshold proved to result in the most optimal detection with minimum false positive and false negative rates. The use of tools such as Process Monitor, Wireshark, and ProcDOT proved effective in identifying ransomware behavior. However, it should be noted that ProcDOT cannot directly visualize file encryption activity.

APPENDIX

1. Table IX is the calculation of Accuracy, Precision, Recall, and F1-Score at the threshold tested using Confusion Matrix.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 2056-2068

TABLE IX
CALCULATION OF ACCURACY, PRECISION, RECALL, AND F1-SCORE

Threshold	**TP** (TRUE POSITIVE)	**FP** (False Positive)	**TN** (True Negative)	**FN** (False Negative)
50%	2	3	1	0
60%	2	1	3	0
70%	1	0	4	1
80%	0	0	4	2
69%	2	0	4	0

a. 50%
- Akurasi = $\frac{2+1}{2+1+3+0} = \frac{3}{6} = \frac{1}{2} = 50\%$
- Precision = $\frac{2}{2+3} = \frac{2}{5} = 40\%$
- Recall = $\frac{2}{2+0} = \frac{2}{2} = 100\%$
- F1-Score = $2\ x\ \frac{40\ x\ 100}{40+100} = 57\%$

b. 60%
- Akurasi = $\frac{2+3}{2+3+1+0} = \frac{5}{6} = 83{,}3\%$
- Precision = $\frac{2}{2+1} = \frac{2}{2} = 100\%$
- Recall = $\frac{2}{2+0} = 100\%$
- F1-Score = $2\ x\ \frac{100\ x\ 100}{100+100} = 100\%$

c. 70%
- Akurasi = $\frac{1+4}{1+4+0+1} = \frac{5}{6} = 83{,}3\%$
- Precision = $\frac{1}{1+0} = \frac{1}{1} = 100\%$
- Recall = $\frac{1}{1+1} = \frac{1}{2} = 50\%$
- F1-Score = $2\ x\ \frac{100\ x\ 50}{100+50} = 66{,}6\%$

d. 80%
- Akurasi = $\frac{0+4}{0+4+0+2} = \frac{4}{6} = 50\%$
- Precision = $\frac{0}{0+0} = 0\%$
- Recall = $\frac{0}{0+2} = \frac{0}{2} = 0\%$
- F1-Score = $2\ x\ \frac{0\ x\ 0}{0+0} = 0\%$

e. 69%
- Akurasi = $\frac{2+4}{2+4+0+0} = \frac{6}{6} = 100\%$
- Precision = $\frac{2}{2+0} = 100\%$
- Recall = $\frac{2}{2+0} = \frac{2}{2} = 100\%$
- F1-Score = $2\ x\ \frac{100\ x\ 100}{100+100} = 100\%$

REFERENCES

[1] A. Arabo, R. Dijoux, T. Poulain and G. Chevalier, "Detecting Ransomware Using Process Behavior Analysis," *Procedia Computer Science,* pp. 290-296, 2020.

[2] K. Thummapudi, P. Lama and R. V. Boppana, "Detection of ransomware attacks using processor and disk usage data," *IEEE,* pp. 51395 - 51407, 2023.

[3] T. R. Reshmi, "Information security breaches due to ransomware attacks - a systematic literature review," *International Journal of Information Management Data Insights,* vol. 1, 2021.

[4] N. Hampton, Z. Baig and S. Zeadally, "Ransomware behavioural analysis on windows platforms," *Journal of Information Security and Applications,* vol. 40, pp. 44-51, 2018.

[5] D. W. Fernando, N. Komninos and T. Chen, "A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques," *Lecture notes in computer science,* vol. 1, no. 2, pp. 551-604, 2020.

[6] S. Zollner and K.-K. R. Choo, "An Automated Live Forensic and Postmortem Analysis Tool for Bitcoin on Windows Systems," *IEEE Access,* vol. 7, pp. 158250-158263, 2019.

[7] M. . E. Russinovich, D. A. Solomon and A. Ionescu, Windows Internals Part 2, Redmond: Microsoft Press, 2012.

[8] L. Chappell, Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide, Carmel: Chappell University, 2017.

[9] C. Miess, "ProcDot: The Malware Analysis Tool," CERT.at, 05 April 2013. [Online]. Available: https://www.procdot.com. [Accessed 10 Januari 2024].

[10] K. K. Z. M. W. &. M. W. Cabaj, "Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics," *Journal of Network and Computer Applications,* vol. 66, pp. 353-368, 2018.

[11] BBC News Indonesia, "BSI diduga kena serangan siber, pengamat sebut sistem pertahanan bank 'tidak kuat'," BBC News Indonesia, 16 Mei 2023. [Online]. Available: https://www.bbc.com/indonesia/articles/cn01gdr7eero. [Accessed 08 Januari 2024].

[12] Y. Lemmou and J. Lanet, "A behavioural in-depth analysis of ransomware infection," *IET Information Security,* vol. 15, no. 1, pp. 38-58, 2020.

[13] F. De Gaspari and D. Hitaj, "Evading behavioral classifiers: a comprehensive analysis on evading ransomware detection techniques," *Neural Computing and Applications,* vol. 34, no. 14, pp. 12077-12096, 2022.

[14] M. A. Ferrag, O. Friha and L. Maglaras, "Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis," *IEEE Access,* vol. 9, pp. 138509-138542, 2021.

[15] S. Gulmez, A. G. Kakisim and I. Sogukpinar, "Analysis of the Dynamic Features on Ransomware Detection Using Deep Learning-based Methods," *IEEE Access,* 2023.

[16] G. Karantzas and C. Patsakis, "An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors," *Journal of Cybersecurity and Privacy,* vol. 1, no. 3, pp. 387-421, 2021.

[17] Z.-G. Chen, H.-S. Kang, S.-N. Yin and S.-R. Kim, "Automatic Ransomware Detection and Analysis Based on Dynamic API Calls Flow Graph," *Proceedings of the International Conference on Research in Adaptive and Convergent Systems,* vol. 196 , pp. 196-201, 2017.

[18] S. Jamalpur, Y. S. Navya, P. Raja, G. Tagore and . G. R. K. Rao, "Dynamic Malware Analysis Using Cuckoo Sandbox," *IEEE Access,* 2018.

[19] "Sysmon - System Monitor," Microsoft Docs., 23 07 2024. [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.. [Accessed 15 08 2024].

[20] "Tcpdump/Libpcap public repository," Tcpdump, [Online]. Available: https://www.tcpdump.org/. [Accessed 15 08 2024].

[21] "The Volatility Foundation - Promoting Accessible Memory Analysis Tools Within the Memory Forensics Community," Volatility, [Online]. Available: https://www.volatilityfoundation.org/. [Accessed 15 08 2024].

[22] J. A. H. Silva, L. I. B. López and Á. L. V. Caraguay, "A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters," *Remote Sens,* vol. 11, no. 10, p. 1168, 2019.

[23] D. Kirat, G. Vigna and C. Kruegel, "Barecloud: bare-metal analysis-based evasive malware detection," *USENIX Security Symposium,* pp. 287 - 301, 2014.