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 [12].

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 [13].

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 [14]. 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 [15]. 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 [16].

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 [17]. 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 [18].