Jurnal E-Komtek
Vol. 9, No. 1. (2025) pp. 302-312
https://jurnal.politeknik-kebumen.ac.id/index.php/E-KOMTEK
p-ISSN : 2580-3719 e-ISSN : 2622-3066

Ransomware Attack Analysis in Cybersecurity

Stefanus Eko Prasetyo[1] , Heru Wijayanto Aripradono, Ricardo[3]

[1-3]Department of Information Technology, Universitas Internasional Batam, Indonesia, 29426

2132044.ricardo@uib.edu

https://doi.org/10.37339/e-komtek.v9i1.2279

Published by Politeknik Piksi Ganesha Indonesia

Artikel Info
Submitted:
11-01-2025
Revised:
12-05-2025
Accepted:
26-05-2025
Online first :
30-06-2025

Abstract

Ransomware attacks have emerged as a significant threat to computer security in the digital age. This research aims to analyze ransomware attacks within the context of cybersecurity, specifically focusing on the impact of such attacks on an organization's database infrastructure. The study involves simulating ransomware attacks using techniques commonly employed by attackers in real-world scenarios. It includes a comprehensive literature review, case observations of previous ransomware attacks, and system simulations to understand the nature of these attacks and their potential consequences. The research highlights the need for effective mitigation strategies to safeguard critical organizational infrastructure and provide insights into strengthening defenses against ransomware. The findings of this study are expected to contribute to the development of more effective and sustainable cybersecurity strategies to address the growing complexity of cyber threats and ensure the operational continuity of organizations.

Keywords: *Ransomware attacks, Cybersecurity, Database infrastructure*

Abstrak

Serangan ransomware telah muncul sebagai ancaman signifikan terhadap keamanan komputer di era digital. Penelitian ini bertujuan untuk menganalisis serangan ransomware dalam konteks keamanan siber, dengan fokus pada dampak serangan terhadap infrastruktur database suatu organisasi. Penelitian ini melibatkan simulasi serangan ransomware menggunakan teknik-teknik yang umum digunakan oleh penyerang dalam situasi nyata. Penelitian ini mencakup kajian literatur yang komprehensif, observasi terhadap kasus serangan ransomware sebelumnya, serta simulasi sistem untuk memahami karakteristik serangan ini dan potensi dampaknya. Penelitian ini menyoroti pentingnya strategi mitigasi yang efektif untuk melindungi infrastruktur organisasi yang krusial dan memberikan wawasan untuk memperkuat pertahanan terhadap ancaman ransomware. Hasil dari penelitian ini diharapkan dapat berkontribusi pada pengembangan strategi keamanan siber yang lebih efektif dan berkelanjutan untuk menghadapi kompleksitas ancaman siber yang terus berkembang serta memastikan kelangsungan operasional organisasi.

***Kata-kata kunci**: Serangan ransomware, Keamanan siber, Infrastruktur database*

1. Introduction

The development of information technology has brought significant changes in various aspects of life, including in business, government, and society. With the rapid advancement of technology, the digital world has provided convenience and efficiency in various activities. However, along with the benefits offered by technology, threats to cybersecurity have also increased. One of the most alarming threats and a major concern in recent years is ransomware **[1].**

Ransomware is a type of cyber attack designed to encrypt the victim's data, making the data inaccessible unless the victim pays a ransom to the attacker. The phenomenon of ransomware attacks continues to evolve in terms of both frequency and complexity. Attackers exploit system vulnerabilities, psychological manipulation techniques (social engineering), and sophisticated technology to carry out their attacks **[2]**. In this attack, hackers exploit security loopholes in information systems to infect the victim's devices and secretly encrypt the data.

The impact of ransomware attacks is not only financial but can also cause damage to the organization's reputation, halt operations, and even risk public safety. This is especially true when the attack targets critical sectors such as healthcare, banking, and government infrastructure **[3]**. The dependence on strong digital infrastructure makes these sectors prime targets for ransomware attackers, as an attack on these sectors can have much broader and more severe consequences **[4]**.

The increasing sophistication of ransomware attacks makes research on these attacks even more relevant in the context of cybersecurity. As part of the effort to understand and address this threat, it is crucial to identify attack patterns, underlying causes, and their impact on organizations that are targeted. A deep understanding of the attackers' modus operandi, as well as the vulnerabilities they exploit in systems, is essential to designing and implementing effective mitigation strategies. Therefore, this research aims to analyze various aspects of ransomware attacks in the context of cybersecurity, focusing on the potential impacts on an organization's database infrastructure and the mitigation steps that can be taken to minimize the risks and losses caused by these attacks **[5]**.

Through this research, it is hoped that deeper insights can be gained regarding how ransomware works, the techniques used by attackers, and practical recommendations that organizations can apply to strengthen their defenses against this threat. Furthermore, by using

modeling and simulation techniques that reflect real-world attack scenarios, this research aims to provide guidance that will be useful for organizations in reinforcing their security systems and protecting sensitive data and information from ransomware threats. The findings of this study are expected to make a significant contribution to the development of more effective and sustainable cybersecurity strategies to address future challenges and ensure operational continuity amidst increasingly complex threats.

2. Method

Figure 1. Hybrid Analysis Research Method

From the image above, it is explained that the research methodology uses the Hybrid Analysis technique to gather information about the ransomware workflow and its impact on the database **[6].**

A. Observation

This observation will be conducted carefully on several ransomware incidents, collecting data and recording the information obtained from the observations **[7].**

B. Literature Review

The literature review is carried out by gathering, evaluating, and analyzing relevant and available written literature on ransomware and its impact on a database. By doing so, we can critically evaluate and analyze various aspects of how a database can go down as a result of a ransomware attack **[8].**

2.1. Visual Studio

To create a ransomware, a desktop application called Visual Studio is required. Visual Studio is used to design a desktop-based application to create ransomware from start to finish

and make it runnable on a laptop or computer[9]. This software is used to write the source code or programming commands to make the ransomware encrypt the desired files.

2.2. Database

Any type of database can be used, such as Oracle, MySQL **[10]**, MongoDB, etc. The purpose of using database software is to target and understand how ransomware attacks work when they infiltrate the database **[11].**

2.3. Source Code

Figure 2. Source Code for Encrypting Files

The image above shows a snippet of the source code that can recover files that were previously encrypted by ransomware. This code is designed to restore all files in the Desktop, Pictures, and Documents directories. By using this code, files impacted by ransomware will be restored to their original state through a decryption process. Furthermore, files with the (.jcrypt) extension, indicating they have been infected by ransomware, will be deleted and replaced with the successfully decrypted files **[5].**

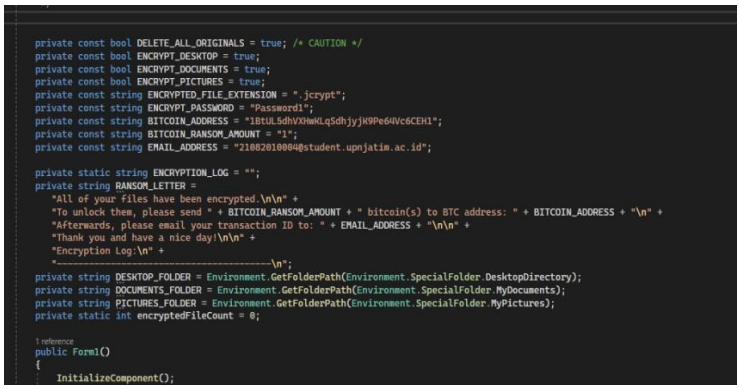

Figure 3. *Source Code for Encrypting Files*

The image above shows a snippet of the source code that will encrypt all files in the Desktop, Pictures, and Documents directories. As a result of ransomware encryption, all files will

be corrupted and inaccessible, as their contents will turn into an unreadable combination of numbers and letters **[2].**

2.4. Implementation of Ransomware Attack Simulation

After creating the ransomware, the next step is to execute the code we have developed. In *Figure 2.4*, the result of the encryption file or encrypt code that has been executed is visible. Then, we wait a moment for the ransomware to work properly and change the targeted files' extensions to .jcrypt **[12].**

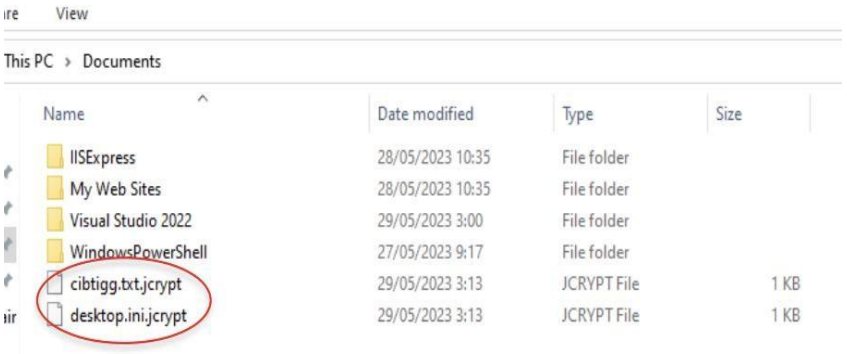

Figure 4. Ransomware Impact on Files

Once ransomware has finished encrypting all targeted files, the display will appear as shown below:

Figure 5. Display of Ransomware Victim

In **Figure 5**, this image will appear, and the victim will receive a warning that all files on their device have been encrypted. To recover the encrypted files, the victim must pay a ransom to the creator of the ransomware. However, paying is highly discouraged because there is no guarantee that the hacker will decrypt the files, and it may create a domino effect, allowing similar incidents to recur as the hacker gains what they want. The solution we recommend is to immediately use anti-malware software such as Windows Defender Anti-Malware **[1].**

Once all the victim's files are encrypted, a recovery file named "recovery file" will appear on the desktop, as shown in *Figure 2.6*. This file serves to inform the victim about the encrypted

files and encourage them to make a payment. Below is an example of the display of files encrypted by ransomware:

Figure 6. List of Files Affected by Ransomware

After the files are encrypted, the victim cannot open them automatically. If they attempt to open the files, random symbols or text will appear, making it unreadable due to encryption, as shown in **Figure 7 [2].**

Figure 7. Contents of a File Affected by Ransomware

Next, we will focus on examining the database display before and after being attacked by ransomware. The goal of this examination is to determine whether the database can still operate or if it has been affected by ransomware. *Figure 2.8* shows an example of the Oracle database display before being attacked by ransomware and before the encryption process **[10].**

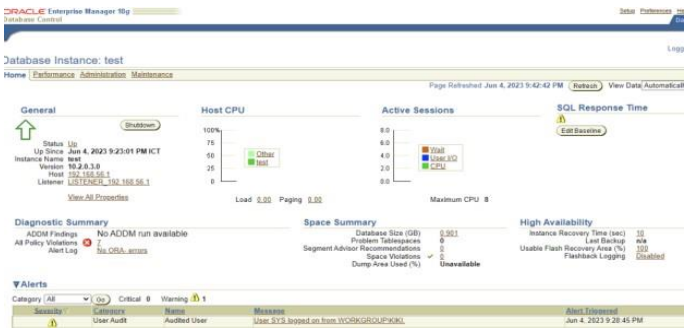

Figure 8. Oracle Database Display Before Ransomware Attack

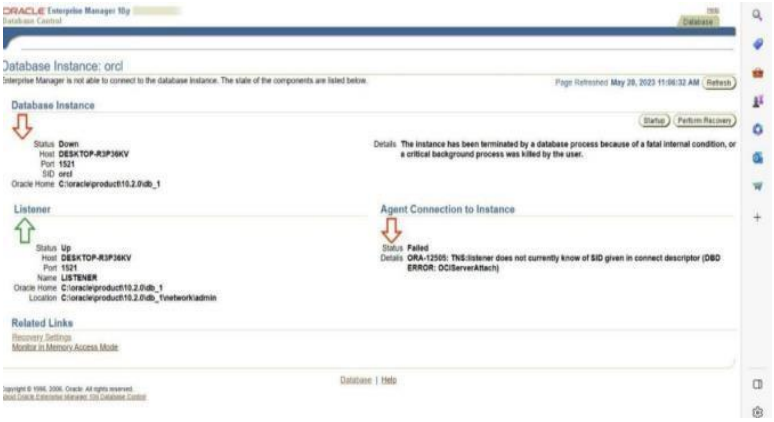

Figure 9. Oracle Database Display After Ransomware Attack

Next, we will observe the Oracle database display after being infected by ransomware and encrypting the data inside, as shown in **Figure 9.** . If we pay attention, there is a difference in the display between the database that is still functioning normally and not infected by ransomware, and the database that has been attacked by ransomware. In the functional database, the display shows the "up" status, indicating that the database is running and ready to accept connections and execute user requests. However, in the database infected by ransomware, the display shows the "down" status, indicating that the database is inactive or not running. When the Oracle database is in "down" status, the instance and background processes do not run, and the database is unavailable to receive connections or execute user requests. Therefore, it can be concluded that the database is likely infected by ransomware **[6].**

2.5. Data Protection in the Database

To mitigate the impact of ransomware on the database, several steps can be taken. One of them is performing regular and scheduled database backups **[13]**. This is important so that when the main data inside the database is corrupted and inaccessible due to ransomware encryption, the data can be restored[14]. It is also essential to store backup copies in multiple locations, such as the cloud, servers, hardware devices (e.g., memory devices), etc **[15].** This will ensure that backup data is more secure and protected from the risk of loss if one storage location encounters issues. Below are some ways to perform data backup or export on the Oracle database:

A. Determine Directory Path for Storing Backup Files

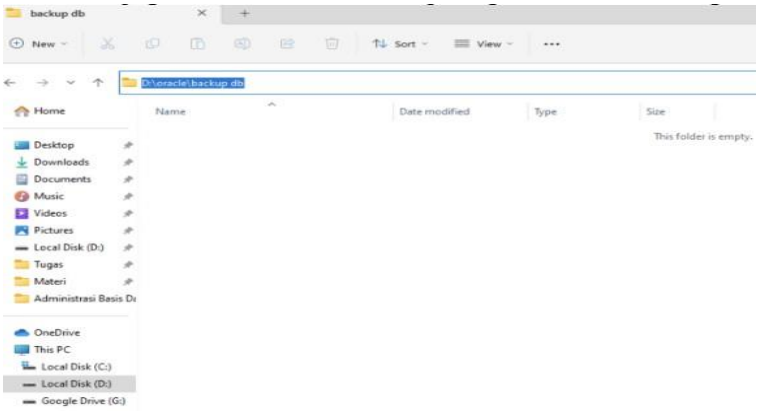

Figure 10. Directory Path for Storing Database Backup Files

Before performing a backup, users will determine the path area created to store the backup files from the primary database, as shown in **Figure 10.**

B. Use Query for Database Backup

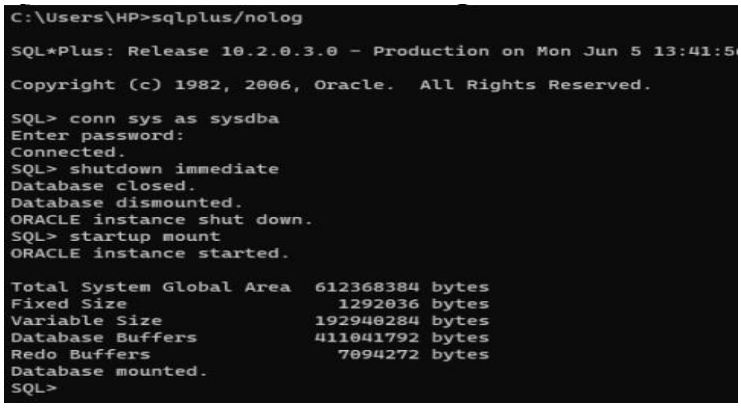

Figure 11. Query to Shutdown the Database

The query shown in **Figure 11.** is used to perform a cold backup, meaning the database is in a shutdown state. The "startup mount" command is used to restart the Oracle database in "mount" mode. This mode allows access to the database control files but does not load the full database, which is necessary before performing a backup **[16].**

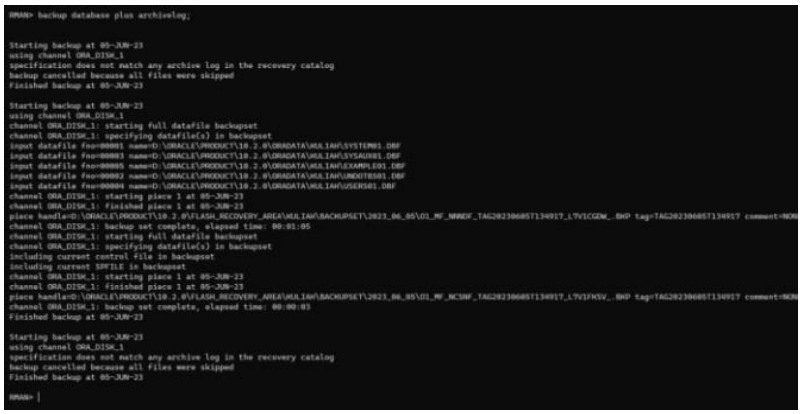

Figure 12. Query for Database Backup

In **Figure 12**, the database backup is performed using the Recovery Manager (RMAN) feature provided by Oracle. The "archivelog" command is used to change the database mode to archivelog mode. This mode allows recording transaction logs into archived logs, which are required for the subsequent complete backup of the database from the last backup point to the next scheduled backup.

3. Result and Discusion

The research results indicate that ransomware attacks have a significant impact on an organization's database infrastructure. In the ransomware attack simulation, we observed how infected files became inaccessible due to the encryption process performed by the ransomware software. The infected files underwent a change in extension to .jcrypt, indicating that the files were locked and could not be opened by users without decryption. Additionally, when ransomware successfully encrypted the database, the database status changed from "up" to "down," signaling that the database was no longer accessible or operational, and services relying on the database were halted.

In the discussion, it is important to note that ransomware attacks can affect various types of databases, such as Oracle, MySQL, and MongoDB, with each type having its own vulnerabilities to such attacks. Therefore, the most effective mitigation strategy is to perform regular backups and store them in separate locations, such as cloud storage or external hardware. The use of anti-malware software, like Windows Defender Anti-Malware, is also recommended to prevent and detect ransomware infections early. Furthermore, this study emphasizes that a more holistic approach to cybersecurity, including early detection, data protection, and rapid recovery, is essential to mitigate the risks posed by ransomware attacks.

4. Conclusion

The rapid development of information technology has led to significant changes across various sectors, including business, government, and society. While it has brought convenience and efficiency, it has also introduced serious cybersecurity threats, particularly ransomware. Ransomware attacks, where cybercriminals encrypt victims' data and demand a ransom for decryption, have become more frequent and sophisticated. These attacks exploit system vulnerabilities and manipulate users through social engineering tactics. The impact of such

attacks is far-reaching, causing not only financial losses but also operational disruptions and reputational damage, especially for critical infrastructure like healthcare, banking, and government systems.

To address this growing threat, this research focuses on understanding the nature of ransomware attacks and their effects on organizational databases. Through a combination of observation, literature review, and simulation of ransomware attacks, the study seeks to identify attack patterns, vulnerabilities, and effective mitigation strategies. One critical recommendation is the importance of regular data backups stored in multiple secure locations, ensuring recovery in case of an attack. The findings from this research aim to provide valuable insights for organizations to strengthen their cybersecurity measures and protect sensitive data from ransomware threats, contributing to more resilient and secure digital infrastructures in the future.

References

[1] B. Hartono, "Ransomware: Memahami Ancaman Keamanan Digital," *Bincang Sains dan Teknologi*, vol. 2, no. 02, pp. 55–62, May 2023, doi: 10.56741/bst.v2i02.353.

[2] A. P. Novita *et al.*, "CYBER SECURITY THREATS; ANALISIS DAN MITIGASI RESIKO RANSOMWARE DI INDONESIA," *Jurnal Simasi : Jurnal Ilmiah Sistem Informasi*, vol. 3, no. 1, pp. 160–169, Jun. 2023, doi: 10.46306/sm.v3i1.

[3] Eka Febriantika Nur Afifah, Diny Widya Evriyanti Simatangkir, and Nafiza Salsabila Faliha, "Afifah et al. - 2025 - KEAMANAN SIBER DALAM PERBANKAN SERTA TANTANGAN DAN," *Multidisiplin Ilmu Akademik*, vol. 2, pp. 1–10, Dec. 2024, doi: https://doi.org/10.61722/jmia.v2i1.3119.

[4] Aryanto Nur and Danang Abu Hafid, "Nur and Hafid - 2024 - PERANAN IT SECURITY DALAM MENGAMANKAN INFRASTRUKTU," *Jurnal Sains dan Teknologi*, vol. 4, pp. 1–20, Oct. 2024, doi: https://doi.org/10.3785/kohesi.v4i10.6528.

[5] D. A. Saputra, S. Deris, and S. Tata, "Implementasi Sistem Deteksi Ransomware Menggunakan Deep Packet Inspection pada Layanan SMK Negeri 1 Palembang," *Indonesian Journal of Multidisciplinary on Social and Technology*, vol. 1, no. 2, pp. 176–183, Jun. 2023, doi: 10.31004/ijmst.v1i2.142.

[6] U. Ubaidillah, T. Taryo, and A. Hindasyah, "Analisis dan Implementasi Honeypot Honeyd Sebagai Low Interaction Terhadap Serangan Distributed Denial Of Service (DDOS) dan Malware," *JTIM : Jurnal Teknologi Informasi dan Multimedia*, vol. 5, no. 3, pp. 208–217, Oct. 2023, doi: 10.35746/jtim.v5i3.405.

[7] A. Afifah Rodhiyatun Nisa, Anandito Daffa Wijayanto, Arya Prabudi Jaya Priana, and A. Setiawan, "Analisis Log Server untuk mendeteksi Serang DDoS pada Keamaan Jaringan di Website," *Journal of Internet and Software Engineering*, vol. 1, no. 3, p. 17, Jun. 2024, doi: 10.47134/pjise.v1i3.2612.

[8] G. Ramadhan, "Ramadhan - 2023 - Perlidungan Hukum Bagi Korban Ransomware Wannacry," *Jurnal Kajian Kontemporer Hukum Dan Masyarakat*, vol. 1, pp. 1–25, Jul. 2023, Accessed: Jan. 10, 2025. [Online]. Available: https://journal.forikami.com/index.php/dassollen/article/view/329

[9] Zahrani Fatni Hapsah and Muhammad Irwan Padli Nasution, "Hapsah and Nasution - 2024 - ANALISIS TINGKAT KEAMANAN DATA PERUSAHAAN YANG REN," *Jurnal Manajemen Dan Akuntansi*, vol. 1, Jan. 2023, doi: https://doi.org/10.62017/wanargi.

[10] T. Kriminologi *et al.*, "JICN: Jurnal Intelek dan Cendikiawan Nusantara Criminology Review of Extortion Crimes Using Viruses, Wannacry Ransomware as a Modern Crime," *Jurnal Intelek dan Cendikiawan Nusantara*, vol. 1, May 2024, [Online]. Available: https://jicnusantara.com/index.php/jicn

[11] B. Brahara, D. Syamsuar, Y. Novaria Kunang, D. Jl Jenderal Ahmad Yani No, S. I. Ulu, and K. Palembang, "Analysis of Malware Dns Attack on the Network Using Domain Name System Indicators Analisis Serangan Dns Malware Di Jaringan Menggunakan Domain Name System Indikator (Studi Kasus Universitas Bina Darma)," *Journal of Information Systems and Informatics*, vol. 2, no. 1, 2020, [Online]. Available: http://journal-isi.org/index.php/isi

[12] Sarvina Sari Ahmad Fadil, "Strategi Pengembangan Sistem Keamanan Terpadu untuk Melindungi Sistem Operasi Windows dari Ancaman Cyber," *Router : Jurnal Teknik Informatika dan Terapan*, vol. 2, no. 3, pp. 122–136, Jul. 2024, doi: 10.62951/router.v2i3.154.

[13] M. Hafeez, A. A. Lubis, and H. Y. Simatupang, "Kerjasama Indonesia-Inggris Dalam Pengembangan Keamanan Siber Nasional Melalui Cyber Diplomacy Indonesia-UK Cooperation in Developing National Cyber Security Through Cyber Diplomacy," 2024. [Online]. Available: http://kti.potensi-utama.ac.id/index.php/globaperspective

[14] A. Dwi Madya, B. Djoko Haryanto, D. P. Ningsih, and F. Sinlae, "Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity," *INDOTECH Indonesian Journal of Education And Computer Science*, vol. 1, no. 3, p. 2023.

[15] E. Dwi Hastri, "Cyber Espionage Sebagai Ancaman Terhadap Pertahanan Dan Keamanan Negara Indonesia," *Law & Justice Review Journal*, vol. 1, no. 1, pp. 12–25, Jun. 2021, doi: 10.11594/lrjj.01.01.03.

[16] Sindy Ariyaningsih, A. Ari Andrianto, Adri Surya Kusuma, and Rina Arum Prastyanti, "Ariyaningsih et al. - 2023 - Korelasi Kejahatan Siber dengan Percepatan Digital," *Jurnal Ilmu Hukum*, vol. 1, pp. 1–11, May 2023, doi: https://doi.org/10.56457/jjih.v1i1.38.