|Jurnal Ilmu Komputer dan Sistem Informasi |JIKSI|Vol. 4| No. 1|Feb|Year 2023|

Virus and Malware Attacks: A Literature Study on Ethical Issues in Information Technology

Celvine Adi Putra[1*]

Abstract

The rapid development of information technology has provided significant benefits for communication, education, and business operations. However, it also introduces serious security and ethical challenges, particularly related to the spread of viruses and malware. This study aims to examine the ethical problems and impacts of virus and malware attacks through a comprehensive literature review. The findings reveal that unethical use of technology, negligence in security practices, and cybercrime motives are major contributing factors to malware proliferation. Ethical awareness, combined with strict cybersecurity policies and user education, is essential in mitigating these risks. This paper contributes to the discourse on digital ethics by emphasizing the shared moral responsibility of users, developers, and organizations in maintaining information integrity and security.

Keywords

Virus, Malware, Ethics, Cybersecurity, Information Technology

Article History
Received 01 October 2022
Accepted 13 January 2023

How to Cite
Putra, C. A. (2023). Virus and Malware Attacks: A Literature Study on Ethical Issues in Information Technology. Jurnal Ilmu Komputer dan Sistem Informasi (JIKSI), 4(1), [1-8].

[1*] Universitas Bina Darama Palembang, Indonesia, Corresponding email: [celvineadiputra@gmail.com]

Introduction

The rapid advancement of information technology has brought remarkable benefits to global society. Today, information and communication technologies are accessible to nearly all social groups without geographical or temporal limitations (Hermawan, 2016). Almost every sector including finance, education, healthcare, politics, and social interaction has adopted information technology to improve efficiency and reach. However, alongside these advancements come new challenges and risks. The development of information technology has opened opportunities for misuse, particularly for criminal activities in cyberspace (Salsabilla Waskita & Sidik, 2023). Cyber threats, such as privacy violations and data breaches, have become increasingly prevalent and can escalate into large-scale cyberattacks. One of the most serious forms of these attacks is malware, which has grown significantly in recent years, posing major risks to user privacy and data security (Fitria, 2023). Malware attacks no longer target only individuals but also extend to large organizations, government institutions, and even national infrastructures.

The diversity and complexity of cybercrime techniques continue to evolve. Attackers often deploy malicious software, commonly referred to as malware, using sophisticated methods to deceive their targets. Malware can spread through various means, including infected applications or downloaded files from compromised websites (Adenansi & Novarina, 2017). The primary objectives of such attacks include surveillance, data theft especially targeting financial information like mobile banking credentials and system disruption. Common malware types include Trojans, viruses, spyware, and exploit-based attacks (Syaputra & Syaifudin, 2020).

Malware, or malicious software, is specifically designed to damage computer systems and programs. It encompasses all harmful software such as viruses, worms, Trojans, ransomware, and spyware (Hama Saeed, 2020). A notable example of malware in Indonesia occurred in 2023, when Bank Syariah Indonesia (BSI) suffered a ransomware attack that disrupted banking services including mobile, internet, and ATM systems for four days, from May 8 to May 11, 2023. The LockBit 3.0 hacker group demanded a ransom of approximately IDR 296 billion to prevent the leak of BSI customer data. When negotiations failed, the attackers released 1.5 TB of confidential data, including personal and employee information of around 15 million customers, on the dark web on May 16, 2023.

The BSI ransomware incident highlights the severe threat malware poses to information systems, as such attacks can result in significant service disruption, data loss, and financial damage. Among various types of malware, the most common are untargeted attacks, which spread indiscriminately by exploiting security vulnerabilities in websites, storage devices, or operating systems (Indana Zulfa et al., 2023). Malware can be categorized into nine groups based on target and attack mechanisms: Backdoor, Downloader, Information-stealing, Launcher, Rootkit, Scareware, Spam-sending, Worm, and Virus (Siddiq et al., 2020; Najoan,

2012; Daniswara et al., 2019). Each type exhibits distinct behaviors, from unauthorized system access to automated propagation and data theft.

Computer viruses, a subcategory of malware, alter or damage files by replicating themselves. Similar to biological viruses, they attach to host programs or files to become active. Viruses typically enter systems through attachments, images, or executable files, performing three main actions: searching for files, replicating themselves, and evading antivirus detection (Dwi Ananto, 2018). Common virus types include Boot sector viruses, File viruses, Resident and Non-resident viruses, Macro viruses, Polymorphic viruses, Metamorphic viruses, and Stealth viruses (Chandini et al., 2019; Dwi Ananto, 2018).

Ethics, as a branch of philosophy, concerns moral principles distinguishing right from wrong and guiding human conduct. It can be divided into general ethics concerned with theoretical foundations and special ethics, which include individual and social ethics. Professional ethics, a subset of special ethics, is closely linked to information technology because it involves understanding professional responsibilities, compliance with regulations, and respect for organizational culture (Wiharto, 2007; Dedes et al., 2022). The rapid and widespread use of technology can bring both benefits and risks; without ethical awareness, it may lead to social problems and negative consequences (Bimantoro et al., 2021). Therefore, ethical considerations form the foundation for responsible use of technology and information.

This article presents a literature study summarizing previous research on virus and malware attacks, their impacts, prevention strategies, and ethical dimensions in information technology. The study also aims to provide a theoretical foundation for understanding the roots of ethical problems, the responsibilities of malware creators, and the social implications of such attacks. Furthermore, it offers insights for future researchers to explore existing knowledge gaps and promote a more comprehensive understanding of ethics in information technology.

Methodology

This research employs a Systematic Literature Review (SLR) approach, which systematically synthesizes existing knowledge and prior studies within the field of information technology. The literature study method allows for identifying, analyzing, and integrating previous research findings, highlighting distinctions, research gaps, and areas of interest (Priharsari, 2022). The SLR process emphasizes a structured and replicable search strategy, evaluation, and synthesis of scholarly works to ensure objectivity and comprehensiveness (Nur Alifah et al., 2023). The purpose of employing this method is to provide a holistic summary of prior findings, identify gaps for future exploration, and ensure methodological rigor (Pakpahan et al., 2021).

The SLR process in this study follows five main stages as described by Samsi Wijaya et al. (2023): (1) research question formulation, (2) search process, (3) inclusion and exclusion criteria, (4) quality assessment, and (5) data collection and synthesis.

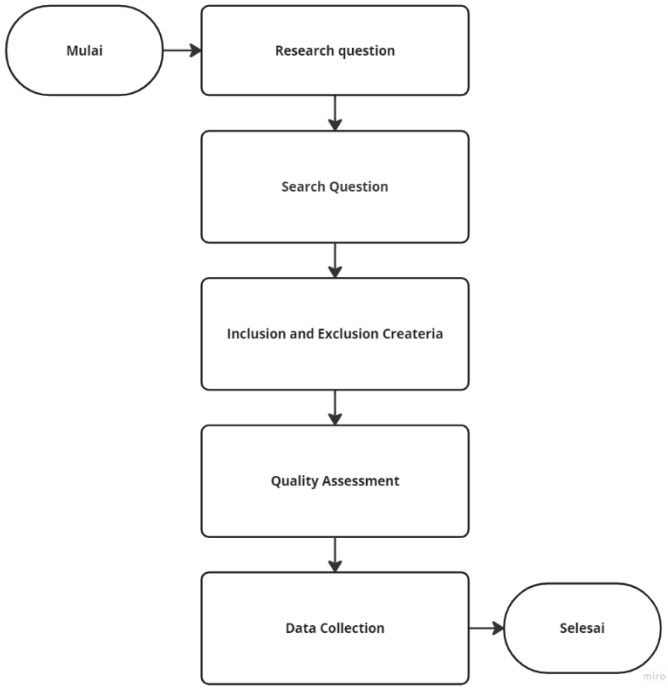

Figure 1: Stages of the Systematic Literature Review Research Method

Results

Journal Search Results

The journal search process was conducted using Publish or Perish software to retrieve articles from Google Scholar within the period of 2019–2024, while international journals were selected manually from reputable databases. The initial search yielded 501 publications from Google Scholar and 10 from international journals, for a total of 511 studies. After screening for accessibility, relevance, and quality, 10 articles were deemed eligible for review.

Discussion Based on Research Questions

This section discusses findings aligned with each research question (RQ):

1. RQ1: Ethical Implications of Virus and Malware Attacks
   The reviewed studies indicate that malware primarily aims to infiltrate systems for theft, manipulation, or surveillance purposes (Naira Fayyaza et al., 2023). Such actions constitute ethical violations related to privacy, integrity, and justice (Dedes et al., 2022). Malware activities disrupt trust and accountability in the digital ecosystem, raising concerns about moral responsibility among developers and users.
2. RQ2: Types of Ethical Issues Arising from Malware Attacks

Ethical problems identified include data theft, identity forgery, deception, and exploitation of user vulnerabilities (Butarbutar, 2023; Soesanto et al., 2023). These behaviors reflect deliberate misuse of technology for personal or organizational gain, violating the ethical principles of beneficence and non-maleficence.

3. RQ3: Ethical Countermeasures and Prevention Strategies
   The literature highlights multiple prevention strategies such as awareness training, legal reinforcement, and adoption of AI-based detection systems (Connolly et al., 2020; Jobair Hossain Faruk et al., 2022). Furthermore, ethical governance frameworks and digital literacy programs are recommended to strengthen cybersecurity culture within institutions and society.

Summary of Literature Findings

No	Study Title	Author(s)	Main Findings
1	Maintaining Digital Rights in the Open Era	(Naira Fayyaza et al., 2023)	Malware targets data manipulation and privacy breaches
2	The Role of Ethics in Information Technology	(Dedes et al., 2022)	Cyberattacks violate moral and legal principles
3	Cybersecurity in Fintech	(Anggono & Riskiyadi, 2021)	Data loss and identity exposure in financial systems
4	Cybercrime Against Individuals	(Butarbutar, 2023)	Identity forgery and fraud activities
5	Cybersecurity Improvement Analysis	(Soesanto et al., 2023)	Online fraud and credit card data theft
6	Ransomware Threats	(Naira Fayyaza et al., 2023)	Financial loss and operational disruption
7	Empirical Study of Ransomware	(Connolly et al., 2020)	Organizational vulnerabilities and recovery costs
8	AI Techniques for Malware Detection	(Alawida et al., 2022)	AI enhances malware detection capabilities
8	Malware Detection and Prevention using Artificial Intelligence Techniques	(Jobair Hossain Faruk et al., 2022)	AI enhances malware detection capabilities
9	Machine Learning for Malware Detection	(Sharma & Arora, 2020)	Data mining supports proactive prevention
10	Anti-Virus Prevention Techniques	(Rohith & Kaur, 2021)	Use of antivirus tools for risk reduction

Discussion

Overall, the synthesis shows that ethical issues in malware attacks revolve around the violation of privacy, misuse of technology, and lack of accountability. The literature confirms that ethical frameworks combined with technological innovation are critical in addressing modern cybersecurity challenges. Furthermore, machine learning and artificial intelligence represent emerging ethical and technical tools for proactive malware detection and prevention.

Conclusion and Recommendations

Based on the findings of this study, which employed a systematic literature review method, it is evident that research addressing the ethical dimensions of cyberattacks—particularly those involving viruses and malware—remains limited. The reviewed literature reveals several major ethical violations, including breaches of privacy, user security, and data integrity. These violations often manifest as identity theft, data manipulation, and fraudulent use of personal information, leading to significant financial, reputational, moral, and social harm.

Current legal and policy frameworks governing cybercrime in Indonesia have not yet been implemented optimally. As noted by Indah and Sari (2021) and Rokhman and Liviani (2020), the challenges stem from legal inconsistencies, inadequate law enforcement, limited infrastructure, and insufficient public awareness. These factors hinder effective cybercrime mitigation and allow the frequency of malware attacks to continue rising.

To address these issues, preventive and ethical approaches are required. Users and organizations should adopt basic cybersecurity practices, such as using licensed software, installing updated antivirus tools, and maintaining cautious digital behavior. From a research perspective, future studies should explore advanced malware detection methods, including machine learning and artificial intelligence approaches, to enhance the ethical and technical frameworks of cybersecurity defense systems.

Disclosure Statement

No potential conflict of interest was reported by the authors.

Acknowledgments

This research was supported by Universitas Bina Darma, Palembang, Indonesia. The author expresses gratitude to the academic supervisors and colleagues from the Master of Informatics Engineering Program for their insights and collaboration.

References

Abdulloh, M. (2019). Analisis penyebaran malware pada sistem informasi berbasis jaringan. Jurnal Ilmu Komputer dan Teknologi Informasi, 7(2), 101–108.

Al-Awadi, M., & Renaud, K. (2021). Ethical responsibility and employee awareness in cybersecurity. Information and Computer Security, 29(3), 379–397. https://doi.org/10.1108/ICS-12-2020-0182

Arifin, A., & Rahmawati, D. (2021). Analisis penyebab kebocoran data pada sistem keamanan siber. Jurnal Teknologi Informasi dan Komputerisasi, 9(2), 45–53.

Babu, A., Singh, S., & Kumar, R. (2021). Malware detection and analysis: Emerging trends. Journal of Information Security and Applications, 58, 102776. https://doi.org/10.1016/j.jisa.2021.102776

Floridi, L., & Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374(2083), 20160118. https://doi.org/10.1098/rsta.2016.0118

Karnouskos, S. (2020). The role of trust and ethics in digital security ecosystems. Computer Standards & Interfaces, 70, 103420. https://doi.org/10.1016/j.csi.2020.103420

Nugraha, Y., Fadillah, H., & Supriyono, B. (2023). Cyber ethics and responsibility: Analysis of hacker communities in Indonesia. Jurnal Keamanan Siber dan Etika Digital, 3(1), 12–24.

Pertiwi, R. A., Utami, D., & Hardi, S. (2020). Analisis etika profesi terhadap keamanan data pada sistem informasi. Jurnal Sistem Informasi dan Teknologi Komputer, 5(3), 155–163.

Putri, A. W., Hasan, M., & Rofiq, A. (2022). Analisis serangan ransomware pada sektor pendidikan di Indonesia. Jurnal Teknologi dan Keamanan Informasi, 8(4), 210–221.

Razaq, M., Ahmed, A., & Khan, N. (2020). Ethical hacking and moral dimensions of cybersecurity. International Journal of Ethics and Information Technology, 22(2), 119–132. https://doi.org/10.1007/s10676-020-09543-z

Santoso, F., & Pradana, A. (2022). Tantangan etika dalam keamanan siber di Indonesia. Jurnal Informatika dan Kebijakan Publik, 4(2), 33–44.

Supriyanto, A., Wijaya, I., & Taufik, R. (2023). Analisis perilaku penyebaran virus komputer berdasarkan pendekatan etika digital. Jurnal Rekayasa Teknologi Informasi, 11(1), 55–68.

Yuliana, S., & Yustanti, W. (2019). Analisis serangan virus pada sistem operasi Windows dan pencegahannya. Jurnal Teknologi dan Sistem Informasi, 5(2), 78–85.

Tushir, S., Sharma, S., & Rana, A. (2023). AI-powered malware and defense mechanisms: Ethical and technical perspectives. Computers & Security, 125, 103099. https://doi.org/10.1016/j.cose.2023.103099

Biographical Notes

CELVINE ADI PUTRA is a graduate student at the Master of Informatics Engineering Program, Universitas Bina Darma, Palembang, Indonesia. His research interests include information security, computer ethics, and digital risk management.