DOI: 10.32703/2415-7422-2025-15-1-172-194

UDC 004.056.55: 004.49:004.8

Ahmad Sanmorino*
Indo Global Mandiri University
Jl. Jendral Sudirman No.629 Km.4 Palembang, Indonesia, 30129
E-mail: sanmorino@uigm.ac.id
https://orcid.org/0000-0002-4949-4377

Yatama Zahra
Sriwijaya University
Jl. Palembang-Prabumulih, KM 32 Inderalaya, Kab. Ogan Ilir, Indonesia, 30662
E-mail: green99pasific@gmail.com
https://orcid.org/0009-0000-7285-5399

*(correspondent-author)

The rise of digital threats: A historical perspective on computer viruses and cybersecurity

Abstract. *The rapid evolution of computer viruses has intensified the need for advanced detection mechanisms. This study examines the historical progression of malware and explores the role of machine learning in enhancing cybersecurity defenses. By analyzing major incidents, such as the Morris Worm, ILOVEYOU virus, and WannaCry ransomware, this research highlights patterns in malware development and the increasing sophistication of cyber threats. Findings reveal that traditional signature-based detection methods struggle to keep pace with evolving malware, necessitating a shift toward machine learning-based approaches. Techniques such as anomaly detection, behavioral analysis, and deep learning models have proven effective in identifying previously unseen threats. This study underscores how machine learning enhances real-time threat detection by recognizing subtle patterns and adapting to new attack strategies. Furthermore, the results highlight the challenges of adversarial attacks, where malware is designed to evade detection by manipulating input data. The study emphasizes the need for robust machine learning frameworks capable of resisting such threats. Additionally, integrating AI-driven models with traditional security measures has been shown to improve detection accuracy and response time. By leveraging historical insights and emerging technologies, this research advocates for a proactive approach to cybersecurity. The findings reinforce the importance of continuous advancements in machine learning-driven threat detection to counter increasingly sophisticated cyberattacks.*

Keywords: *machine learning-based detection; cybersecurity threats; anomaly detection; adversarial attacks; malware evolution*

Introduction.

The ever-growing reliance on technology has brought profound changes to modern society but also introduced vulnerabilities that pose significant risks. Computer viruses, once mere experimental tools for programmers, have evolved into sophisticated threats capable of disrupting critical systems, stealing sensitive information, and inflicting financial losses on a global scale (Benmalek, 2024; Sarkar & Shukla, 2023). The pressing issue lies in understanding the historical trajectory of these digital threats to anticipate and mitigate future challenges effectively. This study aims to trace the evolution of computer viruses and their corresponding cybersecurity measures, providing a comprehensive historical perspective that highlights key milestones and lessons learned.

To achieve this, the study adopts a qualitative approach, examining historical data and documented events to explore the motivations, mechanisms, and impacts of notable computer viruses. By employing a historical analysis framework, the study constructs a detailed timeline of these threats while assessing the development of defense strategies over time. Data sources include academic publications, news archives, and case studies that document pivotal incidents such as the Morris Worm, ILOVEYOU virus, and WannaCry ransomware. Through this method, the study unveils patterns that have shaped the cybersecurity landscape (Pärn, Ghadiminia, García De Soto, & Oti-Sarpong, 2024; Sanmorino & Kesuma, 2024). This study contributes to the field by offering a systematic understanding of how past experiences with computer viruses inform current and future cybersecurity practices. By analyzing the motivations behind these threats and the responses they elicited, the study not only highlights the importance of historical context but also provides actionable insights for enhancing digital defenses in an increasingly interconnected world.

The emergence of computer viruses dates back to the early days of computing, with initial examples serving as proof-of-concept experiments rather than malicious tools. For instance, the Creeper virus (1971) demonstrated self-replicating code, inspiring the creation of antivirus software (Ahmad, Bakar, Jan, & Yussof, 2024). Early viruses such as Brain (1986) and the Morris Worm (1988) revealed the potential for widespread disruption, signaling the need for proactive cybersecurity measures. Researchers have extensively documented these incidents, highlighting how the simplicity of early systems allowed relatively straightforward threats to gain global attention.

As the digital landscape evolved, so did the sophistication of viruses and their associated risks. The late 1990s and early 2000s witnessed the rise of viruses exploiting social engineering tactics, such as Melissa (1999) and ILOVEYOU (2000). These attacks demonstrated how human behavior could amplify a virus's reach and impact, leading to significant financial and operational disruptions (Dong, Wang, & Liao,

2016; Gulyás & Kiss, 2023). Scholars in cybersecurity have emphasized the pivotal role of email systems and user awareness in preventing such attacks, underlining the necessity of education alongside technological defenses.

Modern threats, exemplified by Stuxnet (2010) and WannaCry (2017), represent a paradigm shift in the use and purpose of malware (Allegretta, Siracusano, González, Gramaglia, & Caballero, 2025; Rose, Kabban, Graham, Henry, & Rondeau, 2025). These cases highlight the increasing use of viruses as tools for geopolitical and economic manipulation. Researchers have noted the growing complexity of malware, which now targets industrial systems, exploits zero-day vulnerabilities, and uses advanced evasion techniques. These developments underscore the critical need for collaboration between governments, industries, and researchers to build robust, adaptive cybersecurity frameworks capable of addressing these multifaceted challenges.

Literatur Review.

Existing Systematizations of Computer Viruses and Cybersecurity Evolution: The historical documentation of computer viruses and their corresponding defense mechanisms has been a subject of extensive study within cybersecurity research. Scholars have chronicled major cyber threats over the decades, identifying recurring patterns and technological adaptations (Benmalek, 2024; Sarkar & Shukla, 2023). Early studies primarily focused on cataloging prominent viruses, beginning with the self-replicating Creeper virus of 1971, which paved the way for modern malware analysis (Ahmad, Bakar, Jan, & Yussof, 2024). This foundational work established the basis for understanding how malicious programs exploit system vulnerabilities and human behavior to propagate.

As the field matured, researchers broadened their analyses, shifting from virus categorization to an examination of their societal and economic impact. Studies from the late 1990s and early 2000s explored the role of email-borne threats such as Melissa (1999) and ILOVEYOU (2000), demonstrating how social engineering techniques could amplify cyberattacks' reach (Dong, Wang, & Liao, 2016; Gulyás & Kiss, 2023). More recently, investigations into advanced persistent threats (APTs) and state-sponsored cyber warfare, particularly concerning cases like Stuxnet (2010) and WannaCry (2017), have underscored the evolving nature of malware from disruptive nuisances to sophisticated geopolitical tools (Allegretta, Siracusano, González, Gramaglia, & Caballero, 2025; Rose, Kabban, Graham, Henry, & Rondeau, 2025).

Gaps in Current Knowledge: Despite the extensive documentation of computer viruses, certain key gaps remain in the literature. First, while numerous studies have established virus timelines, there is a lack of in-depth analysis connecting historical malware evolution with present-day cybersecurity strategies. Existing research often treats virus development as a linear progression, overlooking the cyclical nature of cyber threats wherein past attack methods resurface in novel forms. This study addresses this gap by tracing historical patterns to better anticipate future cyber threats.

Another significant limitation in current research is the fragmented approach to studying cybersecurity responses. While technical advancements such as antivirus software, intrusion detection systems, and encryption protocols are well-documented, fewer studies comprehensively assess how organizations and governments have adapted to evolving threats over time. The role of global cooperation, regulatory frameworks, and public cybersecurity awareness remains underexplored, despite their increasing relevance in mitigating large-scale cyberattacks (Sanmorino & Kesuma, 2024).

Moreover, existing literature often underestimates the human factor in cybersecurity. While there is recognition of social engineering tactics in malware spread, the psychological and behavioral aspects of cyber hygiene—why users continue to fall victim to phishing emails or fail to update vulnerable systems—have not been sufficiently integrated into malware evolution studies. By incorporating an interdisciplinary perspective that includes human behavior, this study aims to bridge this research gap and offer a more holistic understanding of cybersecurity defense strategies.

Positioning This Work Within the Field: This study builds upon existing research by offering a historically grounded yet forward-looking analysis of computer viruses and cybersecurity. Unlike conventional studies that focus on either malware taxonomy or isolated case studies, this work synthesizes historical data with an analysis of cybersecurity measures to identify long-term patterns and vulnerabilities. By employing a historical analysis framework, this research contextualizes past cybersecurity failures and successes, offering insights that can inform contemporary digital defense strategies. Additionally, this study contributes to the growing discourse on adaptive cybersecurity, advocating for a shift from reactive measures to predictive defense mechanisms. Drawing on past incidents such as the Morris Worm (1988) and WannaCry (2017), this work illustrates how cybersecurity strategies must evolve to counter emerging threats proactively rather than retroactively (Pärn, Ghadiminia, García De Soto, & Oti-Sarpong, 2024; Karki, Hasan, & Sanin, 2024). By integrating technical analyses with behavioral insights, this study reinforces the argument that effective cybersecurity must be a blend of technology, policy, and user education.

In an era where cyber threats are increasingly sophisticated and interconnected, understanding historical cyberattacks is more than an academic exercise—it is a necessity for shaping future defense mechanisms. This study, therefore, serves as a critical bridge between past experiences and future cybersecurity innovations, offering a strategic perspective that policymakers, security professionals, and researchers can leverage to mitigate emerging digital threats.

Research Methods.

To explore *The Rise of Digital Threats: A Historical Perspective on Computer Viruses and Cybersecurity*, this study adopts a qualitative approach, drawing on historical data and documented events that have shaped the evolution of computer

viruses and the corresponding cybersecurity measures. By analyzing past threats and responses, the study aims to provide valuable insights into the trajectory of digital security and the lessons learned along the way.

Approach: This research follows a historical analysis methodology, mapping the timeline of major computer viruses and the strategies developed to counter them. The study examines key malware incidents to understand their impact, motivations, and the countermeasures implemented. This method enables a comprehensive exploration of how cyber threats evolved and how security strategies adapted in response.

Selection Criteria for Viruses: The selection of viruses for this study is based on three key criteria:

Historical Significance – The virus must have played a pivotal role in shaping cybersecurity practices or technological advancements. For example, the Morris Worm (1988) led to the creation of CERTs, influencing global cybersecurity response frameworks.

Impact and Reach – The virus must have caused widespread disruption, financial losses, or institutional response. Notable examples include the ILOVEYOU virus (2000) and WannaCry ransomware (2017), which had significant global consequences.

Diversity in Attack Mechanisms – The study includes different types of malware (e.g., boot sector viruses, worms, ransomware) to illustrate the broad evolution of cyber threats and their adaptation to technological advancements.

Justification for Periodization: To provide a structured historical analysis, the study organizes the evolution of computer viruses into key periods:

Pre-Internet Era (1971-1985) – Viruses primarily existed in isolated environments, spreading through floppy disks and standalone systems.

Early Internet Age (1986-1999) – The rise of networked computers introduced faster-spreading threats, such as email-based macro viruses like Melissa (1999).

The Age of Sophisticated Cyber Threats (2000-2010) – Malware evolved with more destructive capabilities, including the politically charged Stuxnet (2010), demonstrating the potential for cyber warfare.

Modern Cybersecurity Challenges (2011-Present) – The emergence of ransomware, AI-powered attacks, and state-sponsored cyber threats, exemplified by WannaCry (2017) and advanced persistent threats (APTs).

This periodization provides a logical framework to understand how cybersecurity evolved alongside technological progress and digital connectivity.

Data Collection: The study relies on secondary data from multiple authoritative sources:

Books and Academic Papers – Historical accounts and technical analyses of malware.

News Archives and Reports – Documentation of significant cyber incidents, such as the ILOVEYOU and Stuxnet cases.

Technology Websites and Blogs – Insights from cybersecurity experts and organizations like Symantec, Kaspersky, and government agencies (Cartwright, Cartwright, & Edun, 2023; Cascavilla, Tamburri, & Van Den Heuvel, 2021).

Official Cybersecurity Reports – Publications from agencies like CERT, NIST, and industry white papers.

Analytical Framework: The collected data will be analyzed through a structured framework that includes:

Chronological Mapping – Organizing events into a structured timeline to highlight key developments in cyber threats and defenses.

Thematic Analysis – Identifying recurring themes such as motivations behind cyberattacks (e.g., financial gain, activism, espionage) and their impact on cybersecurity policies.

Comparative Analysis – Examining early and modern viruses to identify evolving attack patterns, prevention mechanisms, and industry responses (Chng, Lu, Kumar, & Yau, 2022; Irshad & Siddiqui, 2024).

Impact Assessment – Evaluating the broader consequences of major cyber incidents on regulatory policies, technological advancements, and public awareness.

Scope and Limitations: This study focuses on widely reported viruses and cybersecurity advancements, acknowledging that proprietary or unpublished data may introduce some limitations. Additionally, the study does not conduct primary investigations into malware but relies on credible secondary sources.

Expected Outcomes: This research aims to provide a historical overview of cyber threats, illustrating their impact on digital security practices. By tracing the evolution of computer viruses, the study sheds light on the ongoing cybersecurity challenges and the importance of adaptive security measures in the digital age.

Results and Discussion.

The Timeline of Major Computer Viruses.

The journey of computer viruses is a fascinating tale of creativity, chaos, and adaptation. From their humble beginnings as experiments in self-replicating code to becoming tools of global disruption (Kale, Bostancı, & Çelebi, 2024), computer viruses have evolved alongside the technology they target. Each significant virus in history tells a story—not just of technical ingenuity, but also of the changing motivations behind their creation, from pranks and protests to espionage and financial gain.

This timeline explores the key milestones in the evolution of computer viruses, shedding light on how these digital threats operated, the impact they had, and the lessons they taught us about cybersecurity (Fig 1). Through this historical lens, we can better understand the ongoing battle between malicious software and the defenses we build to protect ourselves in an increasingly connected world.

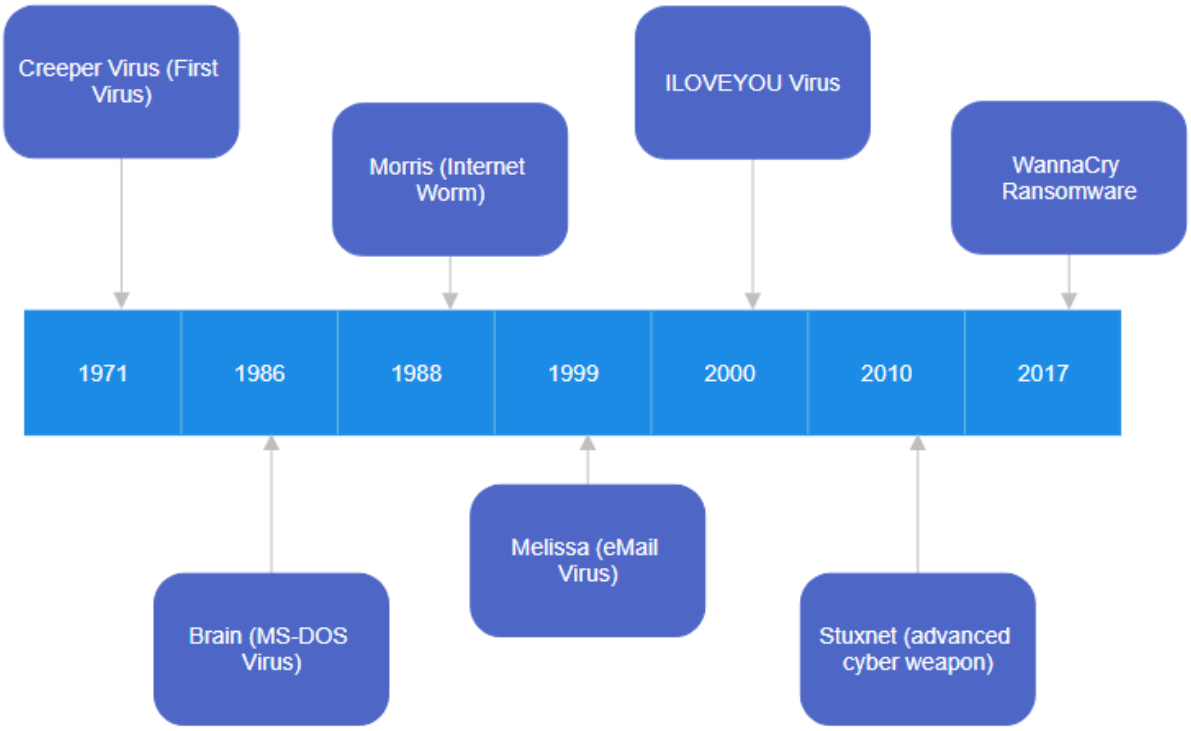

Figure 1. The timeline of major computer viruses (Authors' source).

Creeper Virus (1971): The Creeper virus was the first of its kind, designed not to harm but to demonstrate the concept of a self-replicating program. It worked by hopping between DEC PDP-10 computers running the TENEX operating system. Once it infected a system, it displayed a playful message:

"I'm the Creeper, catch me if you can!"

Instead of causing damage, Creeper replicated itself to other systems, leaving the previous one unharmed. This experiment inspired the creation of the first antivirus, called Reaper, which tracked and removed Creeper.

Brain (1986): Brain was the first MS-DOS virus, created by two brothers in Pakistan to protect their medical software from piracy. It spread by replacing the boot sector of floppy disks with its code, displaying a message with the creators' names and contact details. While Brain wasn't intentionally destructive, it slowed down infected systems and caused confusion, as users were unaware their disks had been altered. Its rapid spread via floppy disks demonstrated the potential of malware to affect systems globally.

Morris Worm (1988): The Morris Worm was the first major internet worm, designed by a computer scientist. It worked by exploiting vulnerabilities in Unix systems, including weak passwords and unpatched software. Once inside a system, the worm replicated itself and spread to other connected systems. Though not intended to cause harm, the worm's replication rate overwhelmed systems, slowing them down or crashing them. This incident highlighted the need for cybersecurity protocols and led to the establishment of the Computer Emergency Response Team (CERT).

Melissa Virus (1999): Melissa was a cleverly designed email virus. It arrived as an email attachment, often titled something enticing like "Important Message." Once opened, it unleashed a macro within a Word document that automatically sent the email to the first 50 contacts in the recipient's address book. Melissa's rapid spread disrupted email servers worldwide, forcing many companies to temporarily shut down their systems. It highlighted the dangers of malicious macros embedded in everyday documents.

ILOVEYOU Virus (2000): The ILOVEYOU virus took social engineering to the next level. It disguised itself as a love letter in an email, with the subject line "ILOVEYOU" and an attachment named "LOVE-LETTER-FOR-YOU.TXT.vbs." Users who opened the attachment activated a Visual Basic script that overwrote files, stole passwords, and spread itself to all email contacts. ILOVEYOU's combination of psychological manipulation and technical damage caused chaos, impacting millions of systems and resulting in billions of dollars in damages. It exposed the risks of opening suspicious attachments and the need for email security training.

Stuxnet (2010): Stuxnet was an advanced cyber weapon, designed to target industrial control systems. Unlike traditional viruses, Stuxnet infiltrated systems through USB drives and exploited multiple zero-day vulnerabilities. Once inside, it reprogrammed industrial equipment to malfunction, specifically sabotaging centrifuges used in uranium enrichment. Stuxnet's precision and stealth were revolutionary. It operated silently, causing physical damage without alerting users, and marked the dawn of malware being used as a tool for geopolitical objectives.

WannaCry Ransomware (2017): WannaCry was a ransomware attack that spread across the globe in hours. It used an exploit in unpatched versions of Microsoft Windows to gain access to systems, encrypting files and locking users out. Victims were shown a ransom note demanding payment to restore their data. The ransomware's rapid spread crippled hospitals, businesses, and public institutions, with damages exceeding $4 billion. WannaCry underscored the importance of timely software updates and the dangers of leaving systems vulnerable.

Table 1 provides a snapshot of some of the most notable computer viruses and malware in history, showcasing their diversity in type, the environments they targeted, and the impact they left behind. From the playful yet groundbreaking Creeper virus in 1971 to the devastating WannaCry ransomware attack in 2017, each entry reflects a turning point in the ever-evolving world of cybersecurity. These viruses not only caused financial losses and operational disruptions but also pushed the boundaries of innovation—on both sides of the cyber battlefield.

The evolution of computer viruses, as reflected in the table, highlights how their complexity and impact have grown over the decades. Early examples, such as the Creeper virus in 1971, were experimental and harmless, serving as a technical demonstration rather than a malicious threat. However, by the mid-1980s, viruses like Brain began exploiting vulnerabilities in floppy disks, marking the start of viruses spreading globally.

Table 1. The Most Notable Computer Viruses in History

Virus Name	Type	First Reported /Outbreak	Environment	Impact or Loss
Creeper	Experimental Virus	1971	Mainframe Computers	First proof-of-concept virus; no financial loss.
Brain	Boot Sector Virus	1986	PCs (Floppy Disks)	Slowed PCs; raised awareness of global virus spread.
Morris Worm	Internet Worm (Alanazi, Mahmood, & Chowdhury, 2023)	1988	Unix Systems	Caused system slowdowns and crashes; $10M in losses.
Melissa	Macro Virus (Rashid, Shafique, Akram, & Elagan, 2024)	1999	PCs (Email Systems)	Overloaded email servers; $80M in damages globally.
ILOVEYOU	Worm/Script Virus (Seshagiri, Vazhayil, & Sriram, 2016)	2000	PCs (Email Systems)	Overwrote files and spread rapidly; $10B in losses.
Stuxnet (Kumar, Govindaraj, Erturk, Nisar, & Inc, 2023)	Industrial Malware	2010	SCADA/ Industrial	Damaged Iran's nuclear facilities; geopolitical impact.
WannaCry (Evans & Purdy, 2023)	Ransomware	2017	PCs (Global Networks)	Crippled healthcare and businesses; $4B in damages.
Mydoom	Email Worm	2004	PCs (Email Systems)	Slowest internet speeds ever; $38B in economic losses.
Zeus	Trojan Malware (Kumar, Shersingh, Kumar, & Verma, 2024; Singh, Krishnan, Vazirani, Ravi, & Alsuhibany, 2024)	2007	Web (Banking Sites)	Stole financial data; billions in stolen funds.
Petya/ NotPetya (Gaber, Ahmed, & Janicke, 2025)	Ransomware	2016/2017	PCs (Corporate Systems)	Disrupted shipping/logistics; $10B in losses globally.

The Morris Worm in 1988 was a wake-up call for internet security, as it disrupted Unix systems and caused significant financial losses, showing the potential for widespread harm when networks were targeted. These early incidents underscored the need for more robust cybersecurity measures and led to the establishment of frameworks like CERT to mitigate future threats (Karki, Hasan, & Sanin, 2024; Kaur, Gabrijelčič, & Klobučar, 2023).

As technology advanced, so did the intent and scope of malicious programs. Viruses such as Melissa and ILOVEYOU in the late 1990s and early 2000s used email systems to propagate, demonstrating how social engineering could amplify their reach and damage. By the 2010s, the stakes were even higher with threats like Stuxnet and WannaCry. Stuxnet showcased malware's ability to physically disrupt critical infrastructure, highlighting its geopolitical implications, while WannaCry exploited network vulnerabilities on a global scale, causing billions in damages. These examples reveal a clear trend: viruses have moved from being curiosities to sophisticated tools capable of devastating financial, social, and political systems. This progression emphasizes the critical need for continuous innovation in cybersecurity to counteract ever-evolving threats.

Figure 2 shows the difference between the old virus mechanism and the modern virus mechanism in a flowchart.

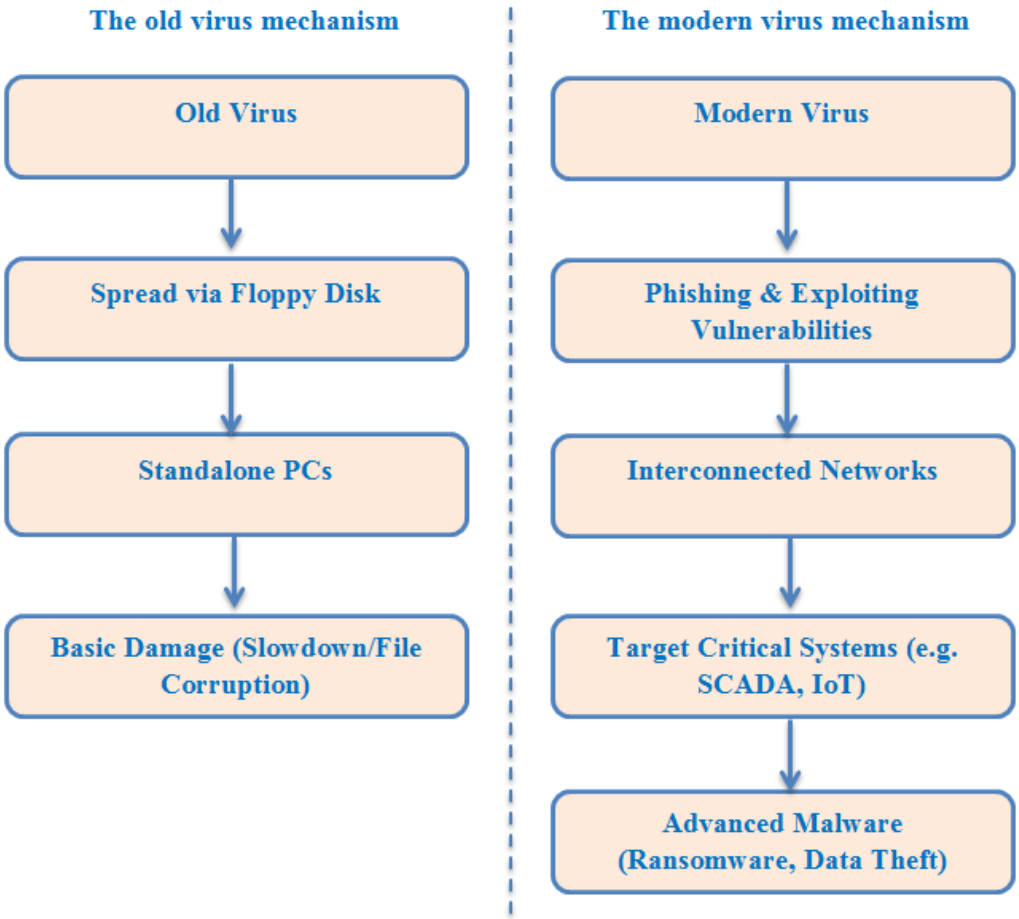

Figure 2. The virus mechanism (Authors' source).

The Figure 2 shows the evolution of computer viruses, contrasting the mechanisms of older viruses with those of modern malware. In the early days, viruses relied on simple distribution methods such as floppy disks. These viruses targeted standalone PCs and were often limited in their impact, causing minor disruptions like slowing down systems or corrupting files. Their functionality was straightforward, reflecting the limited connectivity and less sophisticated systems of that era. These early threats primarily served as proofs of concept or exploratory creations rather than tools for significant harm.

In contrast, modern viruses are far more complex and impactful. They exploit vulnerabilities in interconnected networks, often delivered through phishing attacks or malicious links. Modern malware targets critical infrastructure, including industrial systems and IoT devices, with devastating consequences (Ajay, Nagaraj, Arun Kumar, Suthana, & Ruth Keziah, 2024; Behera, Sahoo, Mishra, & Bhuyan, 2024). Advanced forms such as ransomware and data-theft tools aim for maximum financial or operational disruption, frequently affecting businesses and governments on a global scale. This shift demonstrates how the landscape of cybersecurity has transformed, requiring ever-more advanced defenses to combat these sophisticated threats.

The Virus Mechanisms.

The mechanisms of computer viruses have evolved significantly over time, moving from relatively simple self-replicating scripts to sophisticated cyberweapons capable of large-scale disruption. Understanding these mechanisms in detail—along with their quantitative impact—provides critical insights into their functionality, propagation, and mitigation strategies.

Infection Vectors and Propagation Methods: Viruses and malware spread through multiple mechanisms, each exploiting specific vulnerabilities within a system:

Boot Sector Infection – Early viruses like Brain (1986) replaced the boot sector of floppy disks, altering system initialization. By embedding malicious code within the boot sector, these viruses ensured execution before the operating system loaded. Studies indicate that boot sector viruses affected 5–10% of computers in the late 1980s, particularly in environments with frequent floppy disk exchanges.

Email-Based Transmission – Macro viruses like Melissa (1999) and ILOVEYOU (2000) utilized email attachments, exploiting the widespread use of Microsoft Word macros and Visual Basic scripts. Melissa alone infected an estimated 1 million computers within hours, causing over $80 million in damages. The ILOVEYOU virus escalated this technique, reaching 45 million machines worldwide and leading to an estimated $10 billion in financial losses.

Network Worms and Exploits – The Morris Worm (1988) was among the first to exploit networking vulnerabilities, leveraging weak passwords and Unix sendmail flaws. Modern worms, such as WannaCry (2017), use remote code execution (RCE) exploits like EternalBlue (CVE-2017-0144) to infect

unpatched systems. WannaCry spread to over 200,000 computers in 150 countries within a day, causing $4 billion in damages.

Industrial Control System (ICS) Exploits – Stuxnet (2010) demonstrated the ability of malware to target programmable logic controllers (PLCs) in SCADA systems. The efficiency of Stuxnet's attack underscores how malware can manipulate cyber-physical systems to induce mechanical failures.

Payload Execution and Damage Mechanisms: Once inside a system, viruses deploy payloads with varied effects, categorized as follows:

System Overload and Denial-of-Service (DoS) – The Morris Worm's self-replication mechanism caused excessive CPU and memory usage, slowing systems and rendering them unusable. Modern botnets like Mirai (2016) leverage similar principles, weaponizing IoT devices to execute large-scale DoS attacks exceeding 1 Tbps in traffic volume.

Data Destruction and Manipulation – ILOVEYOU overwrote critical system files and personal documents. In contemporary attacks, ransomware like NotPetya (2017) encrypts entire disk volumes, utilizing AES-128 and RSA-2048 encryption schemes to make data recovery impossible without a decryption key.

Credential Theft and Espionage – Banking trojans such as Zeus (2007) use keylogging and form-grabbing techniques to steal user credentials. Zeus infected an estimated 3.6 million computers in the U.S., resulting in billions of dollars in stolen financial assets. Similarly, APT (Advanced Persistent Threat) malware like Pegasus (2016) exploits zero-day vulnerabilities in mobile devices to conduct state-sponsored surveillance.

Evolution of Defense Mechanisms: As malware sophistication increases, cybersecurity defenses must adapt. The following measures are critical in combating modern threats:

Behavioral-Based Detection Systems – Unlike signature-based antivirus programs, modern endpoint protection platforms (EPPs) use machine learning to identify anomalies. Research suggests that AI-driven malware detection achieves over 97% accuracy in distinguishing between benign and malicious files.

Zero Trust Architecture (ZTA) – Implementing ZTA minimizes unauthorized lateral movement within a network. This approach was instrumental in mitigating the spread of ransomware during the 2021 Colonial Pipeline attack, where network segmentation helped contain damage.

Regular Patch Management – Over 60% of ransomware infections exploit known vulnerabilities that remain unpatched. Organizations must enforce automated patching policies to reduce exposure to threats like WannaCry and EternalBlue.

Multifactor Authentication (MFA) and Least Privilege Access – MFA reduces the risk of credential theft, while least privilege policies limit an attacker's ability to escalate privileges within a compromised system.

Advanced Threat Intelligence and Incident Response – Real-time threat intelligence sharing through platforms like MITRE ATT&CK enhances proactive defense strategies, enabling organizations to anticipate and neutralize emerging threats.

The Motivations.

The motivations behind creating and spreading computer viruses have evolved significantly over time, reflecting changes in technology, societal dynamics, and individual intent. In the early days, many viruses were created out of curiosity or as experiments. As technology advanced and computers became integral to businesses and daily life, the motivations shifted to include financial gain, political activism, and even warfare. Some of the motivations behind viruses are as follows:

Pranks and Mischief: Early viruses were often created for fun or to showcase programming skills. The creators aimed to surprise or amuse others without causing severe damage. The Morris Worm (1988) caused disruptions but was more of an experiment than a malicious act.

Financial Gain: Many modern viruses are created to extort money or steal financial information, targeting businesses or individuals for profit. Ransomware like WannaCry (2017) demanded payments to unlock encrypted files.

Ideological Activism: Hacktivists use viruses to promote political agendas, raise awareness, or protest against organizations or governments. The Anonymous group and politically driven attacks on corporate or governmental networks.

Espionage: Viruses are often used by state-sponsored actors to steal sensitive data, conduct surveillance, or gain competitive advantages. Advanced Persistent Threats (APTs) like those targeting government and corporate secrets.

Sabotage: Malicious software may aim to disrupt critical infrastructure or operations, often for geopolitical or competitive reasons. Stuxnet (2010) was used to sabotage Iran's nuclear facilities.

Revenge: Individuals with grievances against organizations or people may use viruses to damage reputations or operations. Insider attacks involving malware planted by disgruntled employees.

Ego and Notoriety: Some hackers create viruses to gain recognition, prove their technical prowess, or demonstrate vulnerabilities in systems. Early creators like those of the Brain virus (1986) included their names in the code.

Research and Experimentation: Some viruses are created as experiments to understand vulnerabilities and develop stronger cybersecurity defenses. White-hat hackers and researchers sometimes release controlled viruses to test systems.

Accidental Creation: Occasionally, viruses are the unintended result of experiments or poorly designed programs that inadvertently cause harm. Early experimental viruses like Creeper (1971) were not designed to harm but ended up spreading.

Chaos and Destruction: Some creators are motivated purely by a desire to cause widespread disruption without any clear financial or ideological goal.

After learning about the various motivations behind computer viruses, the next step is to explain how to prevent, detect, and mitigate viruses. As the motivations and mechanisms of computer viruses have evolved, so too must our strategies for preventing, detecting, and mitigating them. While some timeless principles remain, the differences between old viruses and modern malware require us to adapt and refine our approaches.

Prevention.

Preventing old viruses was often simpler, as their spread relied on physical media like floppy disks or basic file transfers. The solution was straightforward: avoid using unverified disks, install basic antivirus software, and keep systems updated to close vulnerabilities. These practices were usually enough to thwart most early threats. Modern viruses, however, are far more cunning, often leveraging phishing emails, malicious links, and zero-day exploits. Preventing these requires advanced measures, such as deploying robust email filters, implementing strict patch management to close software loopholes, and educating users about recognizing social engineering tactics. Modern security tools like firewalls and endpoint protection suites further fortify systems against these sophisticated threats.

Detection and Mitigation.

Detection methods for old viruses typically involved scanning files for known virus signatures. These viruses were often repetitive and predictable, making signature-based detection reliable. Simple heuristic techniques also helped identify anomalies in files that had been altered by malware. Modern malware, in contrast, frequently evades traditional detection. Behavioral analysis tools monitor system activities to detect unusual patterns indicative of an attack, while machine learning-powered systems analyze large datasets to predict and identify evolving threats (Dey, Gupta, & Sahu, 2023; Sanmorino, Marnisah, & Kesuma, 2024). Network monitoring tools also play a critical role, scanning for unusual traffic patterns that might signal a breach or ransomware activity. Figure 3 shows the proposed network intrusion detection system (including malicious software, viruses, DDoS attacks, and malware) (Sanmorino, Marnisah, & Kesuma, 2024). The fine-tuned MLP model exhibited strong performance metrics with an average accuracy of 98.5%, precision of 98.1%, recall of 97.8%, and F1 score of 97.9%. These findings demonstrate the model's ability to distinguish between benign and malicious traffic, enhancing network security and resilience.

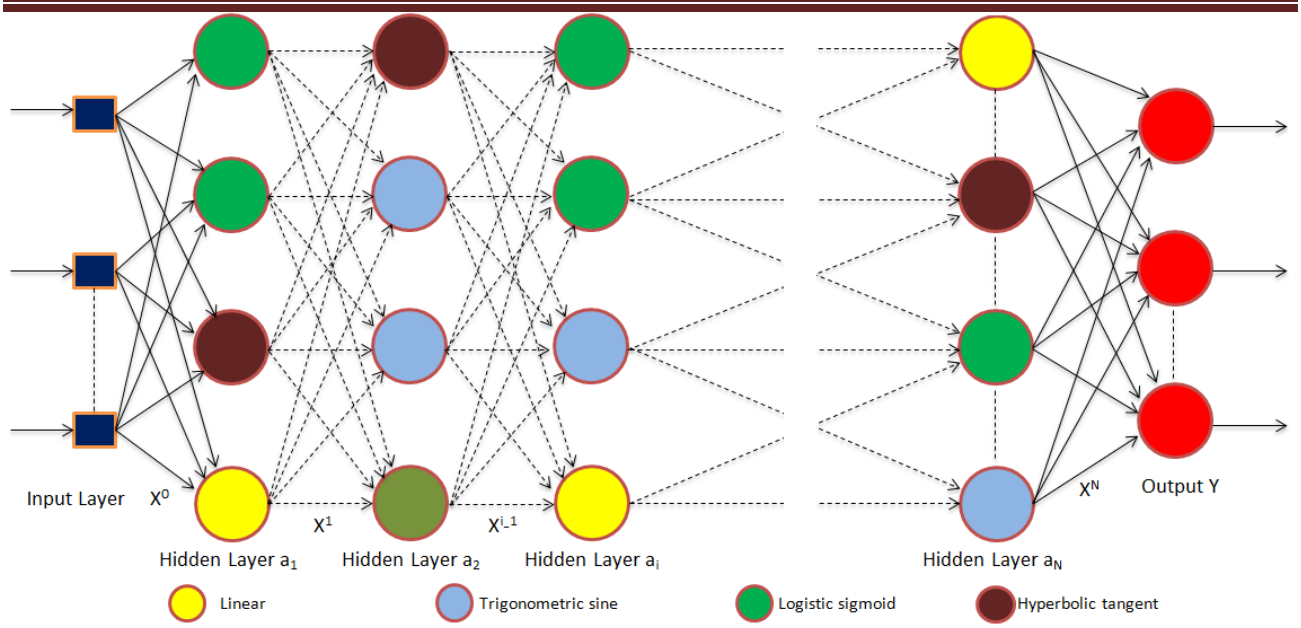

Figure 3. The MLP model architecture for network intrusion detection (Authors' source).

When it came to old viruses, mitigation was relatively straightforward. Infected files could be quarantined and deleted, and in severe cases, the operating system could be reinstalled. Backup systems often sufficed to recover overwritten or corrupted data. Modern viruses require a much more comprehensive approach. For instance, responding to a ransomware attack might involve isolating infected systems, leveraging secure offline backups, and, in some cases, deploying specialized decryption tools. Incident response plans have become essential, providing step-by-step actions to contain and neutralize threats quickly. Threat intelligence sharing with cybersecurity organizations helps mitigate large-scale attacks, ensuring a coordinated response. By understanding the unique characteristics of both old and modern viruses, we can see the importance of adapting our defenses to an ever-evolving landscape.

Future Viruses and AI.

The evolution of computer viruses is expected to accelerate with the integration of artificial intelligence (AI), making future cyber threats more intelligent, adaptive, and stealthy. AI-driven malware is no longer a hypothetical concept—current research and real-world cyberattacks already demonstrate how machine learning (ML) algorithms are being leveraged for malicious purposes (Kazimierczak, Habib, Chan, & Thanapattheerakul, 2024; Kritika, 2025; Sarker, Janicke, Mohsin, Gill, & Maglaras, 2024). As AI-powered cyber threats continue to evolve, understanding these advancements is crucial for cybersecurity professionals (Figure 4).

Initial Development: This is where cybercriminals create the foundation of the AI-powered virus. Using advanced programming, they embed AI algorithms into the malware. These algorithms enable the virus to think and act in a way that traditional malware cannot. Essentially, the virus is designed to learn, adapt, and operate independently, setting the stage for more sophisticated attacks.

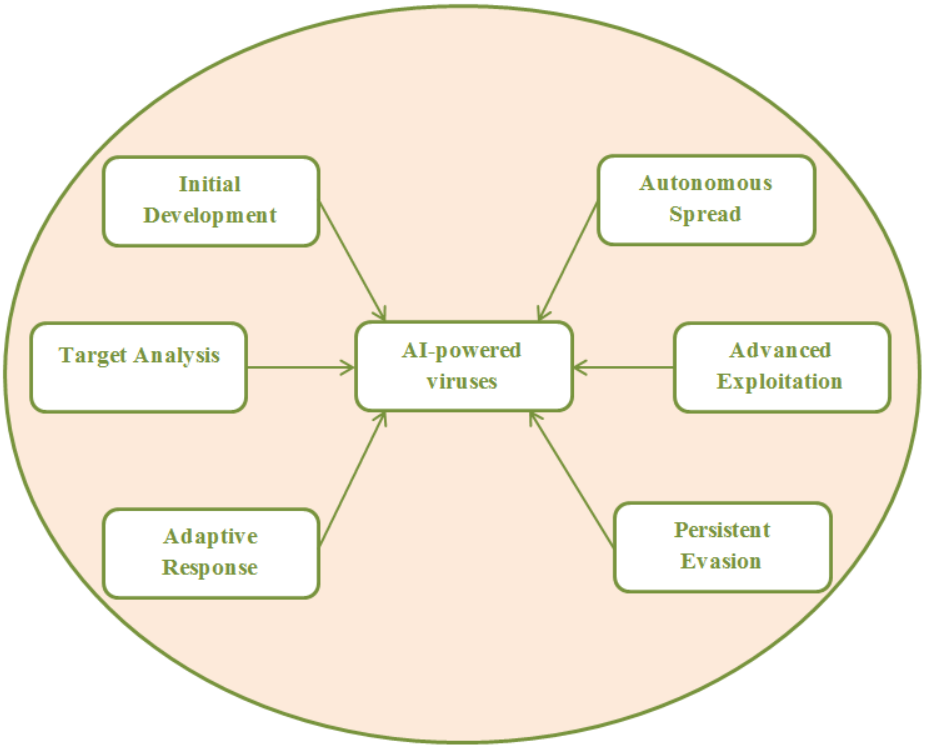

Figure 4. The future virus: AI-powered virus (Authors' source).

Target Analysis: Once deployed, the virus begins analyzing its environment. With AI's help, it gathers data on the target system, such as user behavior, system vulnerabilities, and network activity. For instance, it might observe when users typically access sensitive files or identify weak spots in outdated software. This data allows the virus to create a detailed profile of its target.

Adaptive Response: Here, the AI-powered virus showcases its intelligence. Based on the information gathered during target analysis, it adjusts its behavior dynamically. For example, if it detects that a firewall blocks a specific type of attack, it will shift to a different strategy. This adaptability makes it much harder for traditional security systems to keep up.

Autonomous Spread: Unlike older viruses that require manual triggers or straightforward scripts, AI-powered malware can propagate through networks on its own. It mimics legitimate traffic or activities, blending in to avoid raising suspicion. For instance, it might disguise itself as a regular system update or a harmless email attachment while spreading to connected devices.

Advanced Exploitation: Once inside the system, the virus leverages AI to exploit vulnerabilities with surgical precision. It might use zero-day exploits (previously unknown weaknesses in software) or tailor attacks to specific files, users, or applications. For example, in a corporate network, it could prioritize stealing financial records over less critical data.

Persistent Evasion: The final stage ensures the virus can stay undetected for as long as possible. The embedded AI constantly monitors security tools like antivirus

software or intrusion detection systems (IDS). If it senses it's being analyzed, it adapts by encrypting its code, mimicking legitimate processes, or even deleting traces of itself to throw off defenders.

AI-Driven Attack Mechanisms.

Automated Malware Generation: AI-powered tools such as generative adversarial networks (GANs) have been shown to create highly polymorphic malware capable of continuously modifying its code to evade traditional antivirus detection. This technique was demonstrated in a study where GANs were used to generate malware that bypassed machine learning-based classifiers with a high success rate (Renjith, Sonia, Aji, Corrado, & Vinod, 2022).

Intelligent Target Analysis: AI-powered viruses can analyze massive datasets to identify system vulnerabilities, behavioral patterns, and weak points in network security. For example, the DeepLocker malware, developed as a proof-of-concept by IBM researchers, utilized deep learning to trigger its payload only when specific conditions were met—such as detecting a particular user's face via webcam or identifying specific geolocation markers.

Adaptive Evasion Techniques: Future viruses will employ adversarial machine learning techniques, such as data poisoning and model evasion, to bypass AI-driven cybersecurity defenses. Researchers have already demonstrated how malware can subtly alter its behavior to mislead intrusion detection systems (IDS). A notable example is the use of reinforcement learning to identify and exploit weaknesses in security models, allowing malware to adjust its tactics dynamically.

Autonomous Propagation and Execution: Unlike traditional malware that follows pre-programmed scripts, AI-enhanced viruses will use deep neural networks (DNNs) to autonomously navigate and spread across networks. They will mimic normal user behavior to avoid raising security alerts. The Emotet and TrickBot malware families already incorporate AI-driven techniques to analyze network environments and determine the most effective infection strategies.

Precision Exploitation of Zero-Day Vulnerabilities: AI-driven cyberattacks can leverage deep learning models to scan software for previously unknown vulnerabilities, commonly referred to as zero-day exploits. Researchers at Google's DeepMind have explored the use of AI for vulnerability detection, demonstrating that AI can identify flaws in software code more efficiently than traditional security teams. A real-world example is OpenAI's Codex model, which has shown proficiency in generating and modifying code—including potentially malicious exploits.

Persistent Evasion and Self-Healing Malware: AI-based malware will not only evade detection but also possess self-healing capabilities. By using AI-based mutation engines, future viruses could continuously rewrite portions of their code, preventing detection by behavioral analysis tools. The Houdini malware family has demonstrated early-stage AI-driven evasion by altering attack patterns based on security system responses.

The Potential Impact.

The impact of future viruses could be devastating. Businesses, governments, and individuals could face unprecedented levels of disruption. Imagine ransomware that not only encrypts data but also learns to target backups or AI systems that hijack decision-making processes in critical infrastructure like power grids or healthcare systems. Financial losses could skyrocket as cybercriminals become more efficient at exploiting vulnerabilities. The societal impact could also be profound. Trust in digital systems may erode if AI-powered viruses infiltrate essential services or manipulate information at scale. Cyberwarfare could escalate as nations deploy sophisticated malware against each other, potentially destabilizing geopolitical relations. Furthermore, individuals may face heightened risks to privacy, with viruses capable of harvesting and analyzing personal data in ways never seen before.

Preparing for the Future.

To prepare for this new wave of threats, cybersecurity must evolve alongside them. Organizations and individuals need to adopt proactive strategies that combine human ingenuity with AI-driven defenses. Advanced threat detection systems powered by machine learning will become indispensable, enabling real-time monitoring and analysis of network behavior to identify and neutralize emerging threats. Collaboration across industries and governments will also be crucial. Sharing threat intelligence and investing in cybersecurity research can help develop countermeasures before AI-powered viruses gain widespread traction. At an individual level, fostering a culture of cybersecurity awareness—such as understanding the risks of phishing and securing personal devices—will remain vital.

In essence, while the future of computer viruses will undoubtedly bring new challenges, it also offers opportunities to innovate and strengthen our defenses. By embracing cutting-edge technologies and fostering a united front against these threats, we can prepare for a safer digital future.

Contribution.

This study contributes to the existing body of knowledge by providing a comprehensive analysis of the impact of AI-powered threats on digital security. Unlike previous studies that primarily focused on traditional cyber threats, this research examines the evolving landscape of AI-driven attacks and the necessary countermeasures. Our findings highlight new vulnerabilities introduced by AI systems, emphasizing the need for adaptive security frameworks. Furthermore, we bridge the gap between historical security methodologies and modern AI-enhanced defense strategies. By comparing AI-powered threat vectors with traditional cyberattack patterns, this study offers valuable insights into the shifting nature of cybersecurity challenges. We also propose a predictive model leveraging machine learning techniques to identify emerging threats, improving response time and mitigation

strategies. This research also contributes to policy development by outlining ethical considerations and regulatory measures necessary to address AI-powered cyber threats.

Conclusion.

As computer viruses continue to evolve, becoming more sophisticated and adaptive, our approach to cybersecurity must also advance. From early boot sector infections to AI-driven malware capable of autonomous decision-making, the landscape of digital threats has changed dramatically. Understanding the mechanisms, motivations, and potential impact of these evolving threats is crucial in shaping effective prevention, detection, and mitigation strategies. While modern cybersecurity tools leverage AI and machine learning to counteract emerging threats, the key to resilience lies in proactive defense measures, real-time threat intelligence, and collaboration among industries, researchers, and governments. As we move forward, the battle between cyber attackers and defenders will intensify, making continuous adaptation and innovation essential to safeguarding digital infrastructure and personal security in an increasingly connected world.

Funding.

This research received no external funding.

Conflict of interest.

The authors declare no conflict of interest.

References

Ahmad, I., Bakar, A. A., Jan, R., & Yussof, S. (2024). Dynamic behaviors of a modified computer virus model: Insights into parameters and network attributes. *Alexandria Engineering Journal, 103*, 266–277. https://doi.org/10.1016/j.aej.2024.06.009

Ajay, P., Nagaraj, B., Arun Kumar, R., Suthana, V., & Ruth Keziah, M. (2024). DBN-protected material Enhanced intrusion prevention sensor system defends against cyber attacks in the IoT devices. *Measurement: Sensors, 34*, 101263. https://doi.org/10.1016/j.measen.2024.101263

Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security, 125*, 103028. https://doi.org/10.1016/j.cose.2022.103028

Allegretta, M., Siracusano, G., González, R., Gramaglia, M., & Caballero, J. (2025). Web of shadows: Investigating malware abuse of internet services. *Computers & Security, 149*, 104182. https://doi.org/10.1016/j.cose.2024.104182

Behera, A., Sahoo, K. S., Mishra, T. K., & Bhuyan, M. (2024). A combination learning framework to uncover cyber attacks in IoT networks. *Internet of Things, 28*, 101395. https://doi.org/10.1016/j.iot.2024.101395

Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems, 4*, 186–202. https://doi.org/10.1016/j.iotcps.2023.12.001

Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. *Computers & Security, 131*, 103288. https://doi.org/10.1016/j.cose.2023.103288

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W.-J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security, 105*, 102258. https://doi.org/10.1016/j.cose.2021.102258

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports, 5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Dey, A. K., Gupta, G. P., & Sahu, S. P. (2023). Hybrid meta-heuristic based feature selection mechanism for cyber-attack detection in IoT-enabled networks. *Procedia Computer Science, 218*, 318–327. https://doi.org/10.1016/j.procs.2023.01.014

Dong, T., Wang, A., & Liao, X. (2016). Impact of discontinuous antivirus strategy in a computer virus model with the point to group. *Applied Mathematical Modelling, 40(4)*, 3400–3409. https://doi.org/10.1016/j.apm.2015.10.029

Evans, M., & Purdy, G. T. (2023). Architectural development of a cyber-physical manufacturing range. *Manufacturing Letters, 35*, 1173–1178. https://doi.org/10.1016/j.mfglet.2023.08.124

Gaber, M., Ahmed, M., & Janicke, H. (2025). Zero day ransomware detection with Pulse: Function classification with Transformer models and assembly language. *Computers & Security, 148*, 104167. https://doi.org/10.1016/j.cose.2024.104167

Gulyás, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. *Procedia Computer Science, 219*, 84–90. https://doi.org/10.1016/j.procs.2023.01.267

Irshad, E., & Siddiqui, A. B. (2024). Context-aware cyber-threat attribution based on hybrid features. *ICT Express, 10(3),* 553–569. https://doi.org/10.1016/j.icte.2024.04.005

Kale, G., Bostancı, G. E., & Çelebi, F. V. (2024). Evolutionary feature selection for machine learning based malware classification. *Engineering Science and Technology, an International Journal, 56,* 101762. https://doi.org/10.1016/j.jestch.2024.101762

Karki, S., Hasan, A. B. M. M., & Sanin, C. (2024). Use of ML and AI in cybersecurity-a survey. *Procedia Computer Science, 246*, 1260–1270. https://doi.org/10.1016/j.procs.2024.09.552

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Kazimierczak, M., Habib, N., Chan, J. H., & Thanapattheerakul, T. (2024). Impact of AI on the cyber kill chain: A systematic review. *Heliyon, 10(24),* e40699. https://doi.org/10.1016/j.heliyon.2024.e40699

Kritika, Er. (2025). A comprehensive literature review on ransomware detection using deep learning. *Cyber Security and Applications, 3*, 100078. https://doi.org/10.1016/j.csa.2024.100078

Kumar, P., Govindaraj, V., Erturk, V. S., Nisar, K. S., & Inc, M. (2023). Fractional mathematical modeling of the Stuxnet virus along with an optimal control problem. *Ain Shams Engineering Journal, 14(7)*, 102004. https://doi.org/10.1016/j.asej.2022.102004

Kumar, S., Shersingh, Kumar, S., & Verma, K. (2024). Malware classification using machine learning models. *Procedia Computer Science, 235*, 1419–1428. https://doi.org/10.1016/j.procs.2024.04.133

Pärn, E., Ghadiminia, N., García De Soto, B., & Oti-Sarpong, K. (2024). A perfect storm: Digital twins, cybersecurity, and general contracting firms. *Developments in the Built Environment, 18*, 100466. https://doi.org/10.1016/j.dibe.2024.100466

Rashid, S., Shafique, R., Akram, S., & Elagan, S. K. (2024). New computations of the fractional worms transmission model in wireless sensor network in view of new integral transform with statistical analysis; an analysis of information and communication technologies. *Heliyon, 10(16)*, e35955. https://doi.org/10.1016/j.heliyon.2024.e35955

Renjith, G., Sonia, L., Aji, S., Corrado, A. V., & Vinod, P. (2022). GANG-MAM: GAN based enGine for modifying Android malware. *SoftwareX, 18*, 100977. https://doi.org/10.1016/j.softx.2022.100977

Rose, A. J., Kabban, C. M. S., Graham, S. R., Henry, W. C., & Rondeau, C. M. (2025). Malware classification through Abstract Syntax Trees and L-moments. *Computers & Security, 148*, 104082. https://doi.org/10.1016/j.cose.2024.104082

Sanmorino, A., & Kesuma, H. D. (2024). Fine-tuning a pre-trained ResNet50 model to detect distributed denial of service attack. *Bulletin of Electrical Engineering and Informatics, 13(2)*, 1362–1370. https://doi.org/10.11591/eei.v13i2.7014

Sanmorino, A., Marnisah, L., & Kesuma, H. D. (2024). Detection of DDoS attacks using fine-tuned multi-layer perceptron models. *Engineering, Technology & Applied Science Research, 14(5)*, 16444–16449. https://doi.org/10.48084/etasr.8362

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology, 2*, 100034. https://doi.org/10.1016/j.jeconc.2023.100034

Sarker, I. H., Janicke, H., Mohsin, A., Gill, A., & Maglaras, L. (2024). Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. *ICT Express, 10(4)*, 935–958. https://doi.org/10.1016/j.icte.2024.05.007

Seshagiri, P., Vazhayil, A., & Sriram, P. (2016). AMA: Static code analysis of web page for the detection of malicious scripts. *Procedia Computer Science, 93*, 768–773. https://doi.org/10.1016/j.procs.2016.07.291

Singh, S., Krishnan, D., Vazirani, V., Ravi, V., & Alsuhibany, S. A. (2024). Deep hybrid approach with sequential feature extraction and classification for robust malware detection. *Egyptian Informatics Journal, 27*, 100539. https://doi.org/10.1016/j.eij.2024.100539

Ахмад Санморіно
Університет Індо Глобал Мандірі, Індонезія

Ятама Захра
Університет Шривіджая, Індонезія

Зростання цифрових загроз: Історичний погляд на комп'ютерні віруси та кібербезпеку

Анотація. *Стрімка еволюція комп'ютерних вірусів посилила необхідність у розробці передових механізмів виявлення загроз. Це дослідження розглядає історичний розвиток шкідливого програмного забезпечення та аналізує роль машинного навчання у вдосконаленні засобів кібербезпеки. Аналізуючи ключові інциденти, такі як хробак Morpiса, вірус ILOVEYOU та програма-вимагач WannaCry, дослідження виявляє закономірності у розвитку шкідливих програм та зростаючу складність кіберзагроз. Результати показують, що традиційні методи виявлення, засновані на сигнатурах, не встигають за розвитком шкідливого програмного забезпечення, що зумовлює необхідність переходу до підходів, заснованих на машинному навчанні. Технології, такі як виявлення аномалій, поведінковий аналіз і моделі глибокого навчання, довели свою ефективність у розпізнаванні нових загроз. Це дослідження підкреслює, що машинне навчання підвищує ефективність виявлення загроз у реальному часі завдяки здатності розпізнавати тонкі закономірності та адаптуватися до нових стратегій атак. Крім того, результати висвітлюють виклики, пов'язані з атаками, що використовують методи протидії системам виявлення, коли шкідливе програмне забезпечення навмисно змінює вхідні дані, щоб уникнути розпізнавання. Дослідження наголошує на необхідності розробки стійких до таких атак машинних моделей. Також інтеграція моделей на основі штучного інтелекту з традиційними засобами кібербезпеки покращує точність виявлення загроз і швидкість реагування на них. Використовуючи історичні знання та новітні технології, це дослідження обґрунтовує необхідність проактивного підходу до кібербезпеки. Отримані результати підтверджують важливість безперервного вдосконалення методів виявлення загроз на основі машинного навчання для боротьби з дедалі складнішими кібератаками.*

Ключові слова: *виявлення на основі машинного навчання; загрози кібербезпеці; виявлення аномалій; атаки з використанням протидії; еволюція шкідливого програмного забезпечення*

Received 02.12.2025
Received in revised form 22.02.2025
Accepted 06.03.2025