A method of generating data for further training artificial intelligence models aimed at solving cybersecurity problems*

Ivan Chernihivskyi[1,†] and Larysa Kriuchkova[1,*,†]

[1] Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine

Abstract

Artificial intelligence-based cyberattacks are becoming a significant challenge in cybersecurity. Cybercriminals are using artificial intelligence to increase the sophistication and impact of their attacks, making them increasingly complex and difficult to detect. Threats driven by artificial intelligence can automate vulnerability detection, create convincing phishing schemes, and even adapt in real time to bypass security measures. The dynamic development of artificial intelligence necessitates a proactive and innovative approach to cybersecurity. The paper presents the dynamics of the growth of cybercrime, in particular with the use of AI, and justifies the need to involve AI in solving cybersecurity problems. The method of generating training data for further training AI models proposed, which provides: specialization of a specific AI model to detect the main signs of viral activity in the provided digital traces; improvement of the quality of AI responses; reducing response time to cybersecurity incidents. Presenting digital traces in a tabular format with pre-filtering of digital traces based on a relational artifact table allows reducing the number of elements required for further research.

Keywords

artificial intelligence, neural network models, malware, digital footprints, cyberattacks, cybersecurity, AI model training

1. Introduction

AI-powered cyberattacks are becoming a significant cybersecurity challenge. Cybercriminals are using AI to increase the sophistication and impact of their attacks, making them increasingly complex and difficult to detect. AI-powered threats can automate vulnerability detection, create convincing phishing schemes, and even adapt in real time to bypass security measures. The dynamic development of AI requires a proactive and innovative approach to cybersecurity. Therefore, organizations need to prioritize investments in AI-powered security solutions and constantly improve their strategies to effectively confront rapidly changing threats [1].

Deepfake technology uses artificial intelligence to create realistic fake videos, images, or audio that mimic real people, often making it difficult to identify authentic content. Deepfake is becoming a powerful tool for cybercriminals, as evidenced by the 550% increase in the number of online deepfakes from 2019 to 2023. According to DeepMedia [2], around 500,000 video and voice deepfakes were shared on social media worldwide in 2023. Deepfakes was expected to increase around 8 million by 2025, reflecting the exponential growth of this technology. One of the most prominent examples of this threat is the recent fake photo of a superstar endorsing a politician, after which the superstar explained his opinion and supported another candidate. The widespread availability of advanced artificial intelligence tools and the abundance of publicly available data contribute to the proliferation of deepfakes, making them a significant challenge to cybersecurity efforts [1].

Cybercriminals are already deploying generative AI models to increase the effectiveness and scale of well-known forms of attack, such as ransomware and business email compromise, by

* CPITS-II 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2025, Kyiv, Ukraine

* Corresponding author.

† These authors contributed equally.

i.chernihivskiy@gmail.com (I. Chernihivskiy); alara54@ukr.net (L. Kriuchkova)

0009-0003-4568-3212 (I. Chernihivskiy); 0000-0002-8509-6659 (L. Kriuchkova)

convincingly mimicking the communication styles of company executives through text or video or audio (deepfake) and writing malicious code with AI. GenAI also helps attackers apply social engineering to phishing emails in a wider range of languages [3–5], which expands the attack surface to more people in more countries at lower costs, which in turn allows for more sophisticated and easily scalable cyberattacks [6].

The pace of development of artificial intelligence is constantly accelerating, which has a significant impact on countless industries, and especially on information security [7, 8]. As AI technology has become more accessible to the end user with the introduction of chatbots, attackers have also begun to use this innovative tool, which has led to a significant decrease in the cost and difficulty of detecting cyberattacks. Such misuse of AI technologies is a significant risk, because attackers can easily exploit vulnerabilities in systems, creating problems for security teams [9].

So, if companies want to significantly reduce the impact of cyber threats on their information data, they need to improve protection against deepfake phishing campaigns now by informing staff about the existing threats, investing in protective solutions that involve AI in their work, and implementing AI as one of the components of cyber defense in the enterprise. It should be noted that the time spent in cybersecurity is crucial for detecting and neutralizing threats in the context of malware protection.

The problematic issues of using artificial intelligence in the study of digital traces are outlined in [10], but no specific neural network models or methods for training AI are proposed. We propose a method of generating data for further training AI models in order to improve the quality of solving cybersecurity problems.

2. Research results

Most organizations have formalized a cybersecurity strategy and implemented basic technical controls, such as updated malware protection (77% of organizations), password policies (73% of organizations), network firewalls (72% of organizations), and restricted administrator privileges (68% of organizations). A survey of high ranked executives found that large organizations prioritize cybersecurity more than the others, as shown in Figure 1. While the overall prevalence of cybercrime remained stable, the prevalence of ransomware among organizations increased significantly between 2024 and 2025. The estimated percentage of all organizations that experienced ransomware attacks in the past 12 months increased from less than 0.5% in 2024 to 1% in 2025. Phishing remains the most common type of cybercrime (93% of businesses and 95% of charities have been phished). Businesses that have been victims of cybercrime have experienced an average of 30 cybercrimes of any type in the past 12 months, while charities have experienced 16. This indicates a high level of cyberattacks on the same businesses [11].

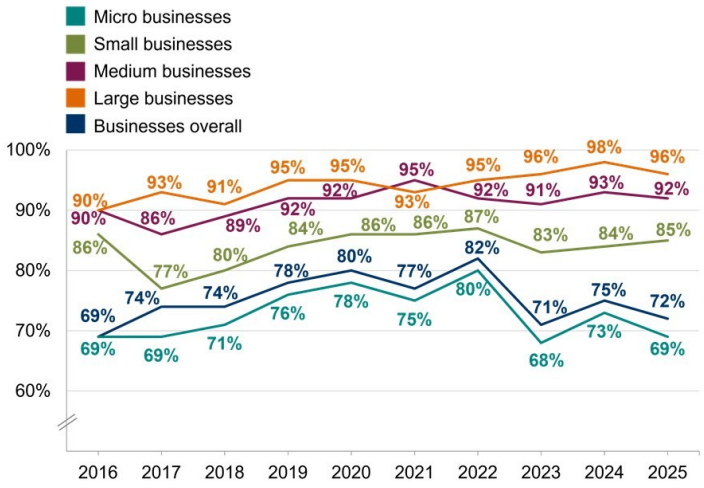

Figure 1: Results of a survey of CEO who consider cybersecurity a high priority [11]

Ransomware attack statistics [12]:

- Ransomware is involved in nearly 70% of malware-related breaches and approximately 24% of all breaches overall.
- The total global cost of ransomware last year exceeded $30 billion.
- According to IBM, the average global cost of a data breach in 2023, including breaches caused by malware, was $4.45 million, a 15% increase compared to 2020.
- For companies with annual revenue of less than $10 million, the average cost of recovering from a ransomware attack is $165,520.
- In 2021, the average demand for ransomware was estimated at $220,298, a 43% increase from 2020.
- According to the FBI, the average amount that ransomware victims paid to the attackers is $10,000.
- In 2023, 84% of private sector organizations affected by ransomware reported revenue loss due to the attack.
- The education sector (94%) and construction sector (93%) most frequently reported business or income losses.

AI engagement statistics [12]:

- Nearly half (46%) of senior security professionals believe that generative AI will increase their organizations' vulnerability to attacks because it can make it easier for attackers to design and execute attacks.
- AI-powered threat intelligence tools boast up to 300% greater accuracy than traditional methods in detecting attempts by malicious scripts to exploit common vulnerabilities targeting a device.
- Artificial intelligence tools can detect 70% more malicious scripts than traditional methods.
- Only 11% of IT managers use AI to detect threats, but 56% are optimistic about its future use.

The growth of cybercrime, including the use of AI, necessitates the use of AI to solve cybersecurity problems. Traditional solutions are still relevant for protection, but organizations urgently need to use and develop their AI to protect their network infrastructure, data, etc. A promising direction is the active use of AI in identifying the state and protecting infocommunication networks to counter cyberattacks, especially those carried out with the involvement of AI, ensuring the detection, analysis and response to cyberthreats in real time and in the future becoming one of the important components of protecting digital systems from new and unknown threats.

In [13], the authors performed a Systematic Literature Review to analyze recent research on LLM4Security and provided a comprehensive mapping of the landscape, identifying how Large Language Models (LLM) are being implemented to improve cybersecurity measures, as depicted in Figure 2. In addition, the authors examined in detail the use of LLMs in different security domains, identifying six main areas corresponding to the topics of the collected articles: software and systems security, network security, information and content security, hardware security, and blockchain security, with a total of 185 articles [13].

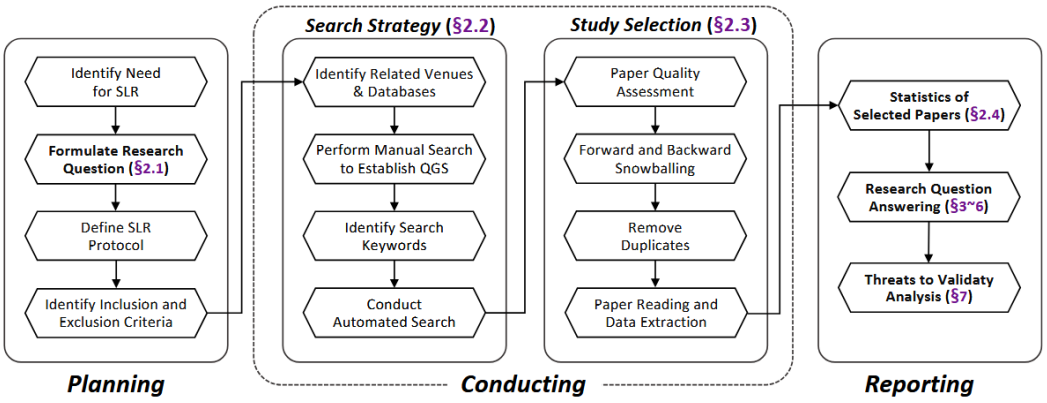

Figure 2: Systematic literature review framework for LLM4Security [13]

In the study [14], a list of possible AI models for use in an infocommunication network to detect viral activity at endpoints based on digital traces is proposed. However, for a better categorization of the PC state as "infected\not infected", it is necessary to retrain any existing AI model on digital traces. The minimum required traces are described in the works [15, 16]. Retraining AI models on digital traces will significantly increase their efficiency compared to undertrained models.

Types of neural network models of artificial intelligence: feedforward neural networks (such as multilayer perceptron); transformers, recurrent neural networks (RNN); convolutional neural networks (CNN); generative adversarial networks (GAN); long short-term memory networks (LSTM) [17]. These models differ in their architecture, the way data is transmitted through them, and specific use cases (Figure 3).

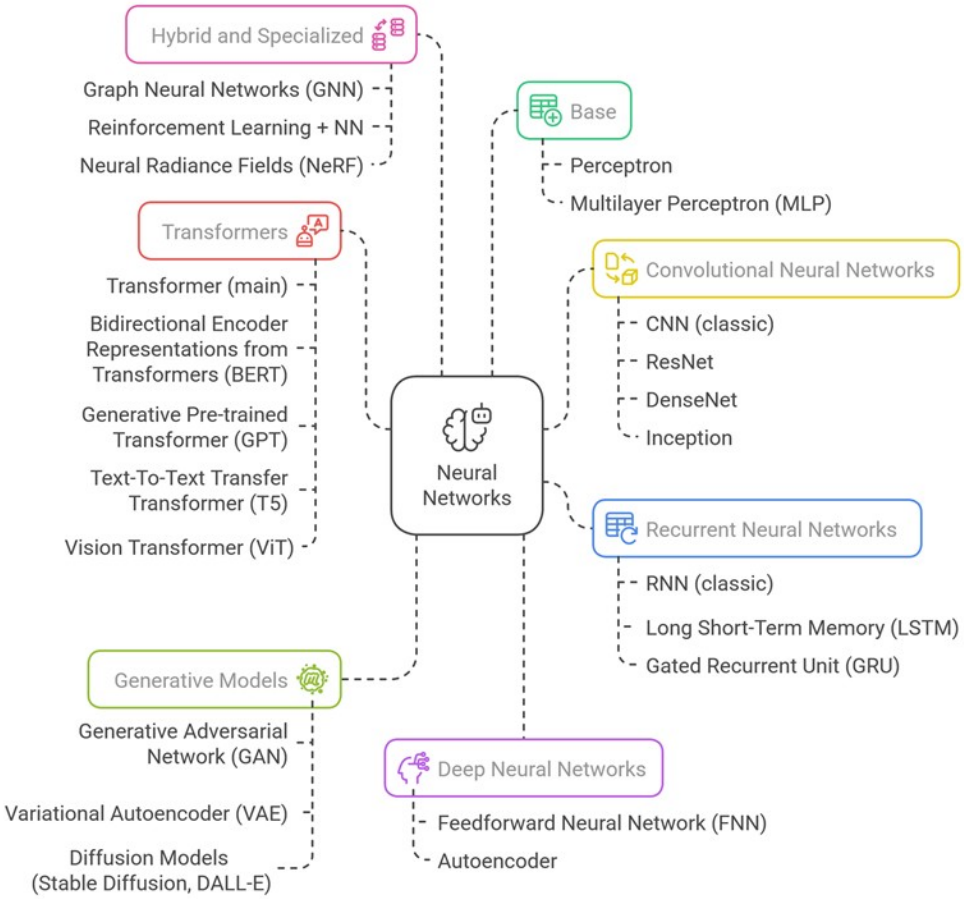

Figure 3: Types of Neural Networks

In all types of machine learning models, the accuracy of the resulting model is highly dependent on the amount and quality of available training data. A model built using an artificial neural network requires more data and resources to train than a traditional machine learning model. This means millions of data points, as opposed to the hundreds of thousands required by a traditional machine learning model [18].

To pre-train or re-train AI models, you need to go through several important steps [19]:

Defining tasks and goals. The tasks that artificial intelligence should solve, as well as specific goals, are defined. It is clearly defined which task needs to be automated or which problem needs to be solved using AI.

Data collection and analysis. The data that will be used to train artificial intelligence is collected and prepared. This may include collecting data from various sources, cleaning it, transforming it, and preparing it for use in the model. Preparing large amounts of data for training AI models is one of the most responsible steps along the way.

Algorithm and model selection. The appropriate algorithm and model are selected to solve the task and achieve the set goals. The choice depends on the characteristics of the task, available data, and required performance. This can be a classic machine learning algorithm, a neural network, or a combination of different approaches.

Model training. The model analyzes the prepared data, identifies patterns, and learns from these patterns, learning to make informed predictions or make decisions. Training can involve an iterative process in which the model is refined and optimized.

Optimization and testing. The model's performance, accuracy, and reliability are tested. The model may be optimized to achieve better results or improve speed.

Implementation and use. After successful testing and optimization, the model is ready to be implemented and used. The model is integrated into an existing system or a special application is created to use it. It is also important to ensure that the model is properly supported and updated so that it continues to work effectively.

Monitoring and improvement. After the model is implemented, it is monitored and continuously improved. Monitoring allows you to track the model's performance in real-world conditions and identify potential problems or the need for changes. Based on the data obtained, adjustments, updates, or retraining of the model can be made to improve its performance.

Therefore, the quality of the prepared data used to train AI models is crucial in solving the tasks that AI models specialize in. Let's consider the listed stages in more detail.

The stage of defining tasks and goals.

The AI model should clearly determine the presence or absence of viral activity based on the provided digital traces, respond Yes\No, and possibly make assumptions about the family of viruses that infected the PC under study.

Data collection and analysis stage.

To obtain digital traces, you must perform the following steps:

1. Prepare a list of malicious software for Windows in .exe format, with a clearly defined family. The only requirement is that the malicious software must perform obvious malicious actions (malicious software that could not be launched due to internal errors is not included in the sample).
2. Prepare a virtual machine (VM) image for VirtualBox that will not have most of the features of a virtual machine [20]. In this case, check the status with the Pafish program with Windows Defender disabled (Figures 4, 5) and use the security recommendations for VMs [21].

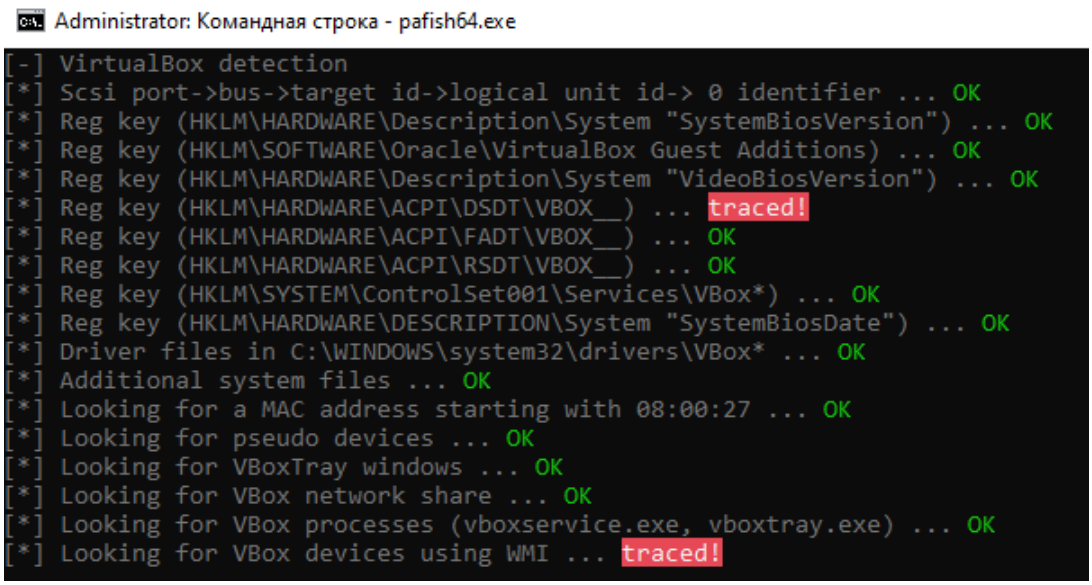

Figure 4: Pafish application window

```
[pafish] Start
[pafish] Windows version: 6.2 build 9200 (native)
[pafish] CPU: GenuineIntel Intel(R) Core(TM) i5-8300H CPU @ 2.30GHz
[pafish] CPU VM traced by checking the difference between CPU timestamp counters (rdtsc) forcing VM exit
[pafish] Sandbox traced by missing dialog confirmation
[pafish] Sandbox traced by missing or implausible dialog confirmation
[pafish] Sandbox traced by checking disk size <= 60GB via DeviceIoControl()
[pafish] Sandbox traced by checking disk size <= 60GB via GetDiskFreeSpaceExA()
[pafish] VirtualBox traced using Reg key HKLM\HARDWARE\ACPI\DSDT\VBOX__
[pafish] VirtualBox device identifiers traced using WMI
[pafish] End
```

Figure 5: Fragment of the Pafish program log

3. Prepare a set of programs for conducting Forensic Triage and an automatic script for launching them [22].
4. Create a user “admin” with administrator rights and a “user” with regular user rights.
5. Update the OS and install all security patches on the VM.
6. Install the following programs:

    - 7-Zip 25.01
    - WinRAR 7.13
    - .NET Framework 2.0, 3.0, 3.5, 4.0, 4.5, 4.8
    - Microsoft .NET SDK 9.0
    - Microsoft Visual C++ Redistributable 2008, 2012, 2013, 2015–2022
    - Microsoft DirectX 9,12
    - Chrome Browser
    - Firefox Browser.

7. Disable Windows Defender on a VM.
8. Collect the minimum necessary artifacts from a clean OS, as a standard [15].
9. Take a VM snapshot (saving the current state of the VM as a “checkpoint” to which you can return at any time) see Figure 6.

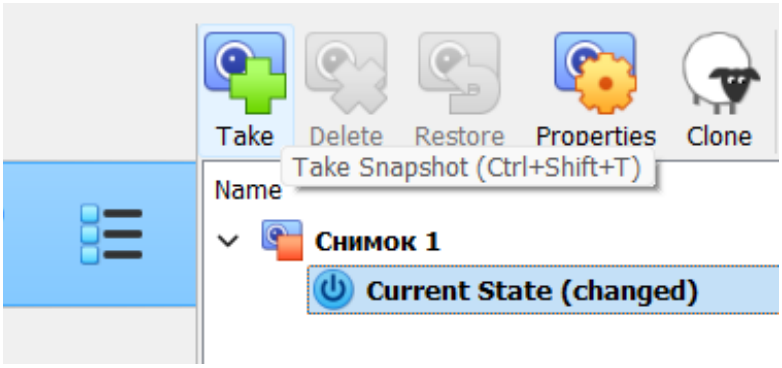

Figure 6: View of the taken snapshot

10. When investigating a malware that has network worm components, the VM should be isolated from the local network by disabling the network adapter using the hypervisor. For all other types of worms, access to the Internet can be left, since the worm can load its modules during operation. If a full investigation of a network worm is necessary, the VM network should be configured to operate in Bridged Adapter mode using the hypervisor, and a separate VLAN should be configured on the router for this VM with access to the Internet and complete lack of access to other segments of the local network, see Figure 7. It is worth noting that there is a possibility that the malware may leave the virtual machine [23] or detect the virtual environment by other signs [24, 25]. In this case, it can be tested on a separate PC, having previously placed it in an isolated VLAN.

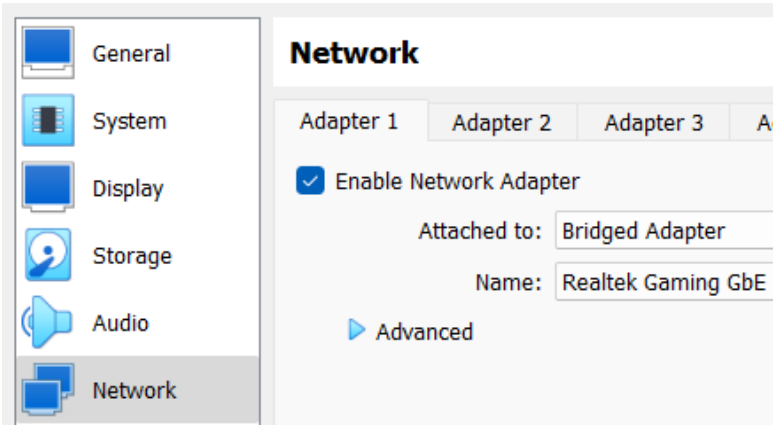

Figure 7: Network adapter in Bridged Adapter mode

11. Upload one malicious instance to a VM.
12. Leave the VM running for about 1 hour (the VM window should be active and the mouse cursor in it should move smoothly), you can reduce this time if you suspect that we will not get more traces.
13. Collect digital traces using the programs prepared in step 3 and upload them to the host machine (PC running the hypervisor).
14. Shut down the VM and restore its state from the snapshot taken in step 9.
15. Repeat steps 10–14 until the list of malwares prepared in step 1 is exhausted.

The result of performing the above 15 steps is to obtain a list of folders and files with digital traces that are inherent in specific instances of the malware. The next task is the need to transform digital traces into a more understandable form for AI. For future model training, it is proposed to format digital traces in a tabular form (see Table 1) with preliminary filtering of digital traces based on the relational table of artifacts presented in [15], which allows reducing the number of elements required for further research.

Table 1
Form of representation of digital traces in the process of further training AI models

Is PC infected?	Malware name	Forensic data
No	-	***Process*** C:\Windows\Explorer.EXE C:\Windows\system32\cexecsvc.exe, C:\Windows\system32\conhost.exe C:\Windows\system32\ctfmon.exe, C:\Windows\system32\DllHost.exe C:\Windows\system32\dwm.exe, C:\Windows\system32\fontdrvhost.exe C:\Windows\system32\lsass.exe, C:\Windows\System32\rdpclip.exe C:\Windows\System32\RuntimeBroker.exe, C: \Windows\system32\sihost.exe C:\Windows\System32\smartscreen.exe, C: \Windows\System32\spoolsv.exe C:\Windows\system32\svchost.exe, C:\Windows\system32\taskhostw.exe C:\Windows\system32\vmcomputeagent.exe, C: \Windows\system32\wbem\wmiprvse.exe, C: \Windows\System32\WindowsPowerShell\v1.0\powershell.exe C:\Windows\system32\winlogon.exe, C: \Windows\System32\WUDFHost.exe C: \Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe, C: \Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe, C: \Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe ***AV Exclusion*** - ***Windows Firewall*** C:\Windows\ehome\ehshell.exe, C:\Windows\ehome\mcrmgr.exe, C: \Windows\ehome\mcx2prov.exe ***Autoruns*** *Known DLLs* c:\windows\system32\wowarmhw.dll, c:\windows\system32\xtajit.dll, c: \windows\system32\xtajit64.dll, c:\windows\syswow64\wow64cpu.dll, c: \windows\syswow64\wowarmhw.dll, c:\windows\syswow64\xtajit.dll, c: \windows\syswow64\wow64.dll, c:\windows\syswow64\wow64base.dll, c:\windows\syswow64\wow64con.dll, c: \windows\syswow64\wow64win.dll, c:\windows\syswow64\xtajit64.dll
Yes	Trojan [Packed] /Win64.Themida Trojan[dropper]: Win/ Tiggre Trojan. Barys	***Hash*** *fa86dd3ccd8ca63f2fa214f43c4d90e09d9e108798952d855b75220e1f207592* ***Process*** C:\ProgramData\RealtekHD\taskhost.exe, C: \ProgramData\RealtekHD\taskhostw.exe, C: \ProgramData\WindowsTask\RealtekHD.exe, C: \ProgramData\WindowsTask\audiodg.exe, C: \ProgramData\WindowsTask\MicrosoftHost.exe ***AV Exclusion***

	C:\Program Files\RDP Wrapper, C:\ProgramData, C: \ProgramData\RealtekHD\taskhost.exe, C:\ProgramData\Windows Tasks Service\winserv.exe, C:\ProgramData\WindowsTasks\AMD.exe, C: \ProgramData\WindowsTasks\AppModule.exe, C: \ProgramData\WindowsTasks\audiodg.exe, : \ProgramData\WindowsTasks\MicrosoftHost.exe, C:\Windows\KMS, C:\Windows\KMSAutoS, C:\Windows\System32 C:\Windows\System32\SppExtComObjHook.dll C:\Windows\System32\SppExtComObjPatcher.exe
	Windows Firewall
	C:\ProgramData\WindowsTasks\AMD.exe, C: \ProgramData\WindowsTasks\AppModule.exe
	Autoruns
	Registry Autorun Entries
	HKLM\Software\Microsoft\Windows\CurrentVersion\Run, Realtek HD Audio, REG_SZ, C:\ProgramData\RealtekHD\taskhostw.exe
	Tasks
	\Microsoft\Windows\WindowsBackup\OnlogonCheck, \Microsoft\Windows\WindowsBackup\TaskCheck C: \ProgramData\RealtekHD\taskhostw.exe \Microsoft\Windows\WindowsBackup\RealtekCheck, \Microsoft\Windows\WindowsBackup\WinlogonCheck C: \ProgramData\RealtekHD\taskhost.exe

The proposed table submission option allows for additional training of the AI model, as it lists the main categories of digital traces without which modern computer viruses usually cannot function normally, the digital traces themselves and the malware that left them, as well as response options for the AI. In addition to virus traces, digital traces from uninfected machines are needed, since the option of mixing the data that will be fed to the AI is being considered.

During AI training at the stage of checking the correctness of the answers, to get closer to reality, it is necessary to mix data with standards where the virus is absent in various combinations of digital traces while preserving the basic structure.

Algorithm and model selection.

The choice of AI model is discussed in detail in [14] and it was concluded that the use of AI models, especially those that have been specially trained for cybersecurity tasks, can already provide acceptable results in determining PC infection based on digital traces, which in turn will increase the speed of response to incidents at the enterprise, however, the final choice of model will depend on the current tasks and available resources.

It will be possible to proceed to other stages after evaluating about 1000 instances using the previously described method. Continuing to perform the analysis of the malicious software using the previously described method and storing the data in such a tabular format allows obtaining high-quality initial data for further training of AI models, which, if sufficient computing resources are available, allows for the specialization of a specific AI model to detect the main signs of viral activity in the provided digital traces, which in turn will increase the quality of AI responses and reduce the response time to cybersecurity incidents (in the case of involving AI in the process of analyzing data from infocommunication networks).

3. Conclusions

Analysis of the dynamics of cybercrime growth, in particular with the use of AI, necessitates the involvement of AI to solve cybersecurity problems.

The proposed method of generating training data for further training of AI models provides: specialization of a specific AI model to detect the main signs of viral activity in the provided digital traces; improvement of the quality of AI responses; reduction of response time to cybersecurity incidents.

Formatting digital traces in tabular form with preliminary filtering of digital traces based on a relational table of artifacts allows reducing the number of elements required for further research.

Further research can be aimed at automating the analysis of AI responses and its integration into cybersecurity systems at the enterprise.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] Top Cybersecurity Threats to Watch in 2025. https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

[2] Deepfaking it: America's 2024 Election Collides with AI Boom. https://www.reuters.com/world/us/deepfaking-it-americas-2024-election-collides-with-ai-boom-2023-05-30/

[3] R. Marusenko, V. Sokolov, I. Bogachuk, Method of Obtaining Data from Open Scientific Sources and Social Engineering Attack Simulation, Advances in Artificial Systems for Logistics Engineering, vol. 135 (2022) 583–594. doi:10.1007/978-3-031-04809-8_53

[4] Z. B. Hu, V. Buriachok, V. Sokolov, Implementation of Social Engineering Attack at Institution of Higher Education, in: 1st Int. Workshop on Cyber Hygiene & Conflict Management in Global Information Networks (CybHyg), vol. 2654 (2020) 155–164.

[5] R. Marusenko, V. Sokolov, P. Skladannyi, Social Engineering Penetration Testing in Higher Education Institutions, Advances in Computer Science for Engineering and Education VI, vol. 181 (2023) 1132–1147.

[6] World Economic Forum: Global Cybersecurity Outlook 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[7] I. Opirskyy, et al. Modern Methods of Ensuring Information Protection in Cybersecurity Systems using Artificial Intelligence and Blockchain Technology. In: O. Harasymchuk (ed.) Kharkiv: Technology Center PC, 2025. doi:10.15587/978-617-8360-12-2

[8] Y. Kostiuk, et al., Models and Technologies of Cognitive Agents for Decision-making with Integration of Artificial Intelligence, in: Modern Data Science Technologies Doctoral Consortium (MoDaST), vol. 4005 (2025) 82–96.

[9] Artificial Intelligence (AI) and Privileged Access Management (PAM) Blog Oberig IT. Oberig IT. https://oberig-it.com/statti/shtuchnyj-intelekt-shi-ta-upravlinnya-pryvilejovanym-dostupom-pam/

[10] Collection "Scientific Bulletin of UzhNU. Series "Law". https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/09/44-3.pdf

[11] Department for Science, Innovation and Technology. Cyber Security Breaches Survey 2025. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025

[12] Malware Statistics: You Need to Know in 2025. https://www.cyberarrow.io/blog/malware-statistics-you-need-to-know/

[13] H. Xu, et al., Large Language Models for Cyber Security: A Systematic Literature Review. doi:10.48550/arXiv.2405.04760

[14] I. Chernihivskyi, L. Kriuchkova, Testing Neural Network Models for Solving the Problem of Detection of Infected PCs based on Digital Traces, Electron. Prof. Sci. Publ. Cybersecurity: Educ., Sci., Technol., 1(29) (2025) 800–817. doi:10.28925/2663-4023.2025.29.941
[15] I. Chernihivskyi, L. Kriuchkova, Effective Solutions for Rapid Detection of Committed PCs in the Infocommunication Networks, Telecommun. Inf. Technol., 87(2) (2025). doi:10.31673/2412-4338.2025.029875
[16] I. Chernihivskyi, L. Kriuchkova, Systematic Approach to Solving the Task of Protecting Information in the infocommunication Network from the Influence of Computer Viruses, Cybersecurity: Educ., Sci., Techn., 2025, 572–590. doi:10.28925/2663-4023.2025.27.781
[17] Y. Kostiuk, et al., Application of Statistical and Neural Network Algorithms in Steganographic Synthesis and Analysis of Hidden Information in Audio and Graphic Files, in: Classic, Quantum, and Post-Quantum Cryptography (CQPC), vol. 4016 (2025) 45–65.
[18] Neural Network Models Explained, Seldon, 2025. https://www.seldon.io/neural-network-models-explained/
[19] How Artificial Intelligence is Created, Lemon School, 2025. https://lemon.school/blog/yak-stvoryuyetsya-shtuchnyj-intelekt
[20] VirtualBox Detection, Anti-Detection, Medium, 2025. https://berhanbingol.medium.com/virtualbox-detection-anti-detection-eng-54a4cde1b509
[21] Chapter 13. Security Guide, VirtualBox, 2025. https://www.virtualbox.org/manual/ch13.html
[22] V. Bilous, et al., Cyber Evidence Software as the Digital Forensics Tools in the Investigation of Cybercrime, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3991 (2025) 26–37.
[23] Sauercl0ud, a2nkf, localo, Escaping VirtualBox 6.1: Part 1, Secret Club, 2021. https://secret.club/2021/01/14/vbox-escape.html
[24] A. Fortuna, Malware VM Detection Techniques Evolving: An Analysis of GravityRAT, 2018. https://andreafortuna.org//2018/05/21/malware-vm-detection-techniques-evolving-an-analysis-of-gravityrat/
[25] VM Detection Tricks, Part 1: Physical Memory Resource Maps, LRQA, 2025. https://www.lrqa.com/en/cyber-labs/vm-detection-tricks-part-1-physical-memory-resource-maps/