BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en

Vol. 29 No. 3. 2024

UDC 004.491
DOI: 10.62660/bcstu/3.2024.10

Malware development: From early viruses to modern cyber threats

Denys Kovalchuk*
Postgraduate Student
International Humanitarian University
65009, 33 Fontanska Rd., Odesa, Ukraine
https://orcid.org/0009-0003-2302-8698

Abstract. Malware is one of the biggest threats in the digital environment, as it is constantly evolving and becoming more dangerous. The purpose of this study was to analyse the evolution of malicious software. Historical, comparative and empirical analysis and an assessment of existing security technologies were used to achieve this goal. The main findings revealed several key stages in the development of malicious software. Historical analysis has shown that the evolution of malware has gone through several significant stages, from simple viruses and worms to complex threats such as ransomware and spyware. These changes were driven by technological advances and increased attack capabilities, which allowed malicious software to use new vectors of influence and deception methods. A comparative analysis of modern cyber threats revealed the key characteristics and differences between different types of malwares, including their specific distribution methods and vulnerabilities. It was found that new threats have a more complex architecture and use more innovative tactics, which significantly complicates their detection and neutralisation. An empirical analysis involving the use of threat detection tools provided specific data on malware behaviour in action. A review and testing of modern security methods, including antivirus solutions, intrusion detection systems, and firewalls, showed their strengths and weaknesses, as well as their effectiveness in detecting and preventing new threats. The results of the study highlighted the need for continuous improvement of protection methods, which is critical for effective control of modern cyber threats

Keywords: evolution of information attacks; digital security; intrusion detection systems; security technologies; computer incident analysis

INTRODUCTION

In today's digital environment, cybersecurity is critical to protecting data and systems from threats and attacks. The theoretical foundations of cybersecurity include understanding the main types of cyber threats, such as malicious software, phishing, ransomware, and ongoing threats of cyber-attacks. Information security principles, including privacy, data integrity, and availability, as well as security techniques such as cryptography, intrusion detection systems, and multi-layer protection, are also important aspects. In the context of rapid technology development and an increase in the number of cyber-crimes, the key aspects are the adaptability of security systems and their ability to quickly respond to new threats. In particular, various organisations and institutions face new challenges, such as the growing complexity of malicious software, infrastructure attacks, and threats to personal data. Existing security systems often do not keep up with the rapid development of attacking methods, which creates significant gaps in information security. These challenges highlight the need for continuous improvement of protection methods and the development of new strategies to effectively counter modern cyber threats. In general, malicious software and attacks, such as ransomware and phishing, are

Article's History: Received: 25.05.2024; Revised 10.08.2024; Accepted 21.10.2024

Suggested Citation:
Kovalchuk, D. (2024). Malware development: From early viruses to modern cyber threats. *Bulletin of Cherkasy State Technological University*, 29(3), 10-20. doi: 10.62660/bcstu/3.2024.10.

*Corresponding author

becoming more complex and adaptive. N. Antonenko *et al.* (2022) investigated current malware detection methods, emphasising the need for new protection mechanisms, which shows the need to improve existing methods. O. Marchenko (2023) analysed the effectiveness of antivirus solutions for critical infrastructure and found that although modern solutions show high results, some security gaps still remain. This confirms the need for further improvements in the protection of critical systems. I. Zulkovska *et al.* (2021) found that none of the existing signature and heuristic methods are perfectly effective, which confirms the need to combine new approaches, such as machine learning and graphical visualisation, to improve the accuracy of threat detection. In turn, the study by I. Galuzin & G. Naiman (2021) showed that vulnerability management technologies, such as Qualys solutions, are effective, but require further improvement and integration with new technologies. In addition, A. Alchi *et al.* (2024) noted that neural networks can significantly improve the accuracy of malware detection by being able to detect patterns in large data sets, although there are problems with the need for significant amounts of training data. This points to gaps in existing methods that require further study. The results of the study by S. Kumar & G. Nagar (2024) emphasised the need for adapted threat models for less developed organisations, which is supported by an analysis of historical incidents and modern sophisticated attacks.

Moreover, M. Qumer & S. Ikrama (2022) examined how artificial intelligence can improve corporate security by detecting and responding to cyber threats. This shows the importance of new technologies in improving security. H.N. Durmuş Şenyapar (2024) emphasised the importance of regular software updates and employee training to improve cybersecurity in digital marketing. The findings of these studies highlight the need for a comprehensive approach to protection that includes both technological and human aspects. The study by P. Ravi *et al.* (2024) demonstrated a machine learning system for detecting ransomware and malware, which indicates the prospects for new approaches in this direction. In addition, R.J. Anderson (2020) analysed current cybersecurity challenges, such as attacks through mobile devices and cloud services, highlighting the need for innovative security solutions. These studies confirm the need for continuous improvement of methods of protection and adaptation to new threats.

Therefore, understanding the evolution of malware is important for improving the level of cybersecurity. Analysis of current research shows that cyber threats continue to evolve, which requires continuous improvement of protection methods and raising awareness of new threats. The purpose of the study was to analyse the evolution of malicious software, and the tasks included identifying the main stages of malware development and evaluating the effectiveness of modern cybersecurity methods.

MATERIALS AND METHODS

For a comprehensive understanding of the evolution of malicious software, a detailed historical analysis was conducted, including the study of its development from initial to modern threats. This analysis examined the first computer viruses and traced their transformation into more complex and diverse types of malicious software. Historical analysis revealed key stages in the development of malware, changes in attack methods and targets, and noted the impact of technological progress on the evolution of threats. This approach involved the analysis of similar scientific studies, which provided a clear picture of how malware technologies and techniques have changed over time.

Next, a comparative analysis of various types of modern cyber threats was carried out, such as viruses (Chernobyl, ILOVEYOU), worms (Blaster, Sasser), Trojans (Zeus, Emotet), rootkits (Stuxnet, Alureon), spyware (Pegasus, CoolWebSearch), botnets (Mirai, Kraken) and ransomware (WannaCry, CryptoLocker). The comparative analysis identified key characteristics and differences between different types of malwares, including their specific distribution methods and vulnerabilities that they use to achieve goals. As part of this analysis, the effectiveness of various methods for detecting and protecting against these threats was also investigated. Various tools and platforms, such as VirusTotal and Cuckoo Sandbox, were used for practical analysis of modern cyber threats. These tools allowed to get data about real-world examples of malicious software programmes, their behaviour, and distribution methods. VirusTotal provided code analysis using various antivirus engines, while Cuckoo Sandbox allowed running data in an isolated environment and investigating its behaviour. Empirical analysis helped to obtain specific data on how malicious software interacts with systems and what protection methods are most effective for detecting and neutralising them.

Evaluation of current malware protection methods included analysis of various technologies and approaches, such as antivirus programmes, intrusion detection systems, firewalls, and user education programmes. Each of these methods was evaluated in terms of its effectiveness in combating modern cyber threats. The study tested and compared antivirus solutions (CCleaner, Norton Antivirus, Bitdefender, McAfee, Avast, TotalAV, Intego, Malwarebytes, Panda), anti-intrusion systems (Snort, Suricata, Malwarebytes, Yara, Hybrid Analysis, ReversingLabs), and firewalls. The evaluation included checking functionality, usability, impact on system performance, and the effectiveness of detecting and preventing new threats. In addition, the role of user education in reducing the risks of cyber threats, including the effectiveness of trainings, was analysed. The results of this assessment helped to formulate recommendations for improving cybersecurity in the face of modern threats.

RESULTS

The evolution of malicious software is one of the most pressing issues in the modern digital world. From the first computer viruses to modern complex cyber threats, the development of malicious software requires constant analysis and the creation of effective protection strategies. In general, the types of malicious software include viruses, worms, trojans, rootkits, spyware, botnets, and ransomware (Fig. 1).

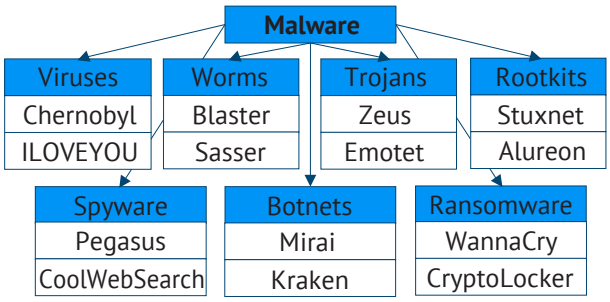

Figure 1. Types of malware and examples
Source: compiled by the author

Viruses are programmes that infect other files and systems by inserting their own code into them. Viruses can self-copy and spread to other computers through infected files. They can corrupt or delete data, slow down systems, or even destroy hardware components. Some viruses can change the functionality of programmes and systems. Worms are self-replicating programmes that are distributed over networks and the Internet, usually without the need for user interaction. They can cause network congestion, system crashes, or use infected devices to attack other systems. In turn, Trojans are programmes that disguise themselves as innocent or useful software, but actually perform malicious actions. They can give attackers access to the victim's system, steal sensitive information, or download other malicious software. Rootkits are a set of tools that allow attackers to gain administrative access to a computer and hide their activities. Rootkits can mask their presence, protect other malicious software from detection, and allow attackers to permanently access the system without the user's knowledge. As for spyware, they collect information about users without their knowledge or consent. Spyware can collect data about personal habits, online activity, passwords, financial information, and other sensitive data. Botnets are networks of infected computers that are centrally controlled to perform malicious tasks. They are used to launch distributed Denial of Service (DDoS) attacks, send spam, steal data, or perform other criminal activities. In addition, ransomware is malicious software that encrypts files on the victim's computer and demands a ransom for decrypting them. Ransomware blocks access to important files or systems and requires payment (usually in cryptocurrency) to restore access. The original malware, such as Creeper and Elk Cloner, appeared in the 1970s and 1980s and had a fairly simple architecture (Matthews, 2022). Creeper, created by Robert Thomas, was one of the first self-copying viruses, and its main purpose was to demonstrate the ability to transfer between computers (Fig. 2). Elk Cloner, created in 1982, was one of the first viruses to infect floppy disks and caused a demo message every 50th system startup.

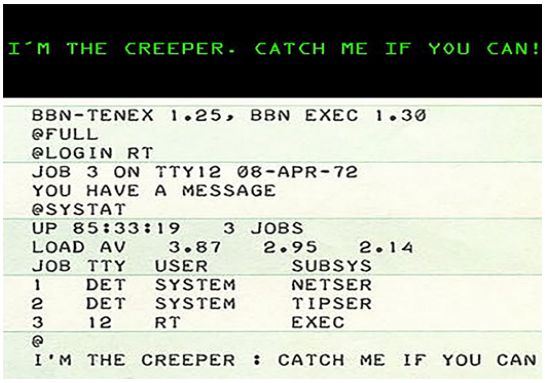

Figure 2. Creeper virus message displayed on infected computers and its source code
Source: compiled by the author

Since the early 1990s, viruses have become more complex. For example, the Chernobyl virus since 1998 included mechanisms that allowed it not only to destroy data, but also to infect the BIOS (Basic Input/Output System) of the computer, which made it difficult to restore the system (Hanna, 2021). Over time, viruses began to use polymorphism mechanisms that made it difficult for antivirus software to detect them by changing their code each time they were launched. Since the 2000s, new types of malicious software have emerged, including Trojans, worms, and rootkits. Blaster and Sasser, which became known in 2003, have demonstrated the ability to quickly spread across networks and exploit vulnerabilities in operating systems (OS) (Karlberg, 2004). These worms exploited vulnerabilities in Windows for their attack, which confirmed the need for regular security updates. Between 2010 and 2020, malicious software underwent significant changes, demonstrating new levels of complexity and technological development. At this time, such types of malwares as ransomware, botnets, and targeted attacks appeared. CryptoLocker, which appeared in 2013, was one of the first ransomware programmes that encrypted files on victims' computers and demanded a ransom in cryptocurrency. Botnets such as Mirai have exploited vulnerabilities in Internet of Things (IoT) devices to create large-scale DDoS attacks that lead to large-scale infrastructure failures. During this period, there was also an increase in targeted attacks on various organisations and state structures. After 2020,

malicious software has become even more complex and specialised. Ransomware attacks such as Conti and DarkSide continue to hit organisations, including critical infrastructure, and require huge amounts in the form of ransomware, often in cryptocurrency (Fig. 3). At the same time, spyware such as Pegasus continues to be used to collect information on mobile devices, in particular, due to vulnerabilities in iOS and Android (Nemchick, 2023). By attacking personal data and communications, these programmes endanger the privacy and security of users on a global level. Consequently, there are a large number of different malicious programmes that continue to evolve with each passing decade, becoming more dangerous, which underscores the need for continuous improvement of cybersecurity technologies.

Modern cyber threats have a significant impact on businesses, individuals, and government agencies. Ransomware causes serious damage by encrypting data and demanding ransom, which can lead to significant financial losses and failures in critical infrastructure. Spyware threatens the privacy of personal data by collecting information without users' knowledge. Botnets can exploit vulnerabilities in IoT to carry out DDoS attacks, leading to large-scale failures in network systems and services. Rootkits allow criminals to mask their presence in the system and collect information without users noticing. Thus, there are many different types of malwares that have significantly changed global security and cyber infrastructure (Table 1). Attacks on critical infrastructure demonstrate how cyber threats can turn into large-scale problems for society. The growing number of DDoS attacks on large service providers and network resources indicates how malicious software can create global disruptions to internet services.

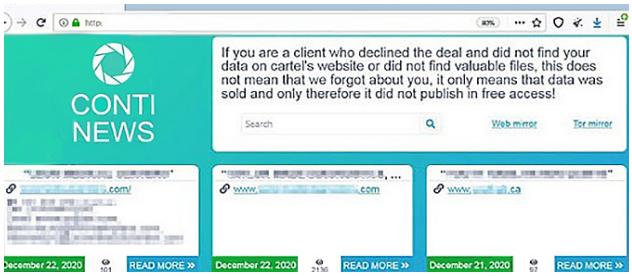

Figure 3. Conti website, where hackers publish stolen data, demanding ransom from victims
Source: compiled by the author based on J. Dalman & H. Smith (2021)

Table 1. Comparison of malware and cyber threats

Type of malware	Main features	Impact on systems
Viruses	Self-copying, infecting files	Data corruption or deletion
Worms	Fast distribution across networks	Network congestion, failures
Trojans	Covert interference, abuse of rights	Data leakage, system compromise
Rootkits	Masking presence, maintaining access	Long-term covert surveillance
Spyware	Collection of information without the user's knowledge	Breach of confidentiality
Ransomware programmes	File encryption, extortion	Loss of access to data, financial losses

Source: compiled by the author

For a better understanding, it is important to consider in detail exactly how malware functions and how they differ. Viruses are attached to files or uploaded to the boot sectors of disks. When an infected file is launched, the virus activates and starts copying its code to other files on disk. This process can spread to other computers if infected files are transferred over networks or specific media. Viruses can cause data corruption, system slowdowns, or even physical damage to hardware components. For example, Chernobyl is a virus that is activated on a specific day and can destroy data on the hard disk and in the computer's BIOS, which makes it difficult to restore the system. ILOVEYOU is a virus that spreads through email and causes numerous infections around the world. In turn, worms exploit vulnerabilities in network protocols or software for self-propagation. They do not require user interaction and often automatically scan networks for vulnerable devices. After finding the vulnerability, the worm infects the device and uses it for further spread. Examples include Blaster, a worm that exploits a Windows vulnerability to spread automatically and cause system crashes, and Sasser, a worm that infects systems through a Windows vulnerability and also causes computers to crash.

Trojans disguise themselves as legitimate or useful programmes that the user can download and install without suspicion. Once installed, the Trojan performs malicious actions, such as giving attackers access to the system, stealing sensitive data, or downloading additional malware. For example, Zeus is a Trojan that steals bank details by replacing web pages to collect login data. While Emotet is a Trojan that gains access to the system and downloads other malicious programmes, stealing data and causing violations in the system. Moreover, rootkits modify the OS or other

applications to hide their presence and activity. They can replace system files or change system settings, making them difficult to detect. Rootkits are often used for long-term monitoring or providing permanent access to the system without the user's knowledge. For example, Stuxnet is a rootkit specifically designed to attack nuclear facilities that modifies control systems to disrupt centrifuges. Alureon is a rootkit that hides other malware and steals data.

Spyware infiltrates the system and collects information about users without their knowledge. They can track online activity, collect input data, collect passwords, browser history, and other sensitive data. There is such a spyware programme as Pegasus, which exploits vulnerabilities in mobile systems to collect personal data and communications. And the CoolWebSearch programme changes the browser settings for collecting information and advertising. There are also botnets consisting of a network of infected devices that are controlled centrally through command servers. These devices can be used to coordinate attacks such as DDoS, sending spam, or data theft. For example, the Mirai botnet exploits vulnerabilities in IoT devices to create large DDoS attacks that cause failures in Internet resources. Kraken is a botnet used to attack websites and send spam.

Ultimately, ransomware encrypts files on the victim's computer and blocks access to them. Next, they demand a ransom to decrypt the data. They usually use strong encryption algorithms, which makes it difficult to recover files without a decryption key. One example is WannaCry, a ransomware that exploits vulnerabilities in Windows to encrypt data and demands a ransom in cryptocurrency. CryptoLocker also encrypts files and requires a ransom to recover them. It turns out that malicious programmes not only complicate conventional methods of protection, but also change approaches to cybersecurity. Attack detection systems such as Intrusion Detection System (IDS) and firewalls must constantly adapt to new forms of threats. The emergence of new types of malicious software requires improved security technologies and increased resources for monitoring and responding to incidents.

Malware monitoring and analysis are critical to ensuring cybersecurity. For this purpose, various tools and platforms were used to help identify, investigate, and respond to cyber threats. Among these tools were VirusTotal and Cuckoo Sandbox, which provide powerful malware analysis capabilities. VirusTotal is a free online service that allows checking files and Uniform Resource Locator (URL) for malicious code using dozens of antivirus programmes and other analysis tools (Fig. 4). When a file is uploaded to VirusTotal, it is checked by various antivirus systems that analyse the file for known malware samples. VirusTotal also provides information about potential threats based on an analysis of the file's behaviour and characteristics.

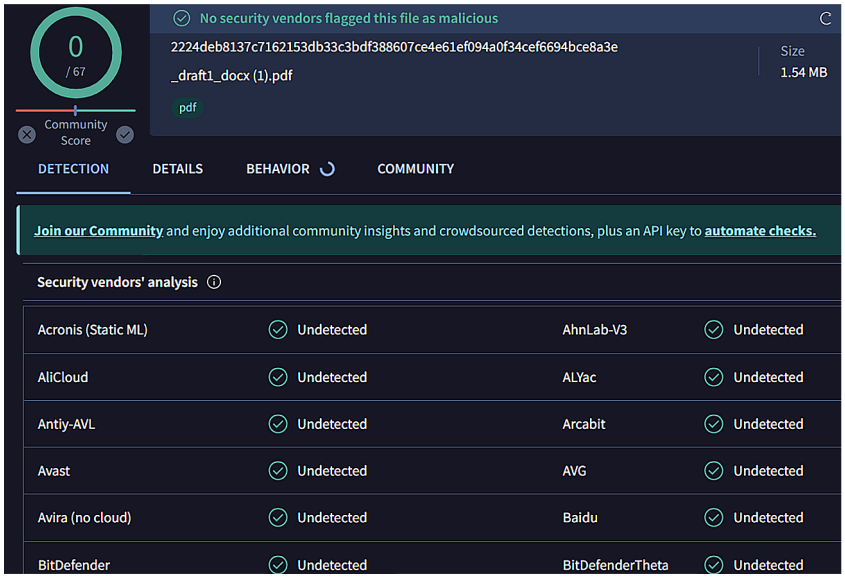

Figure 4. Example of using VirusTotal to check file security

Source: compiled by the author

The Figure 4 shows how the file is sent to VirusTotal, checked by various antivirus systems and analytical tools, and the result is provided to the user. The Cuckoo Sandbox platform is also deserves mentioning, as it is suitable for dynamic malware analysis (Fig. 5). It creates an isolated environment that simulates a real OS, in which malware can be executed to monitor its behaviour. Cuckoo Sandbox collects detailed information about the programme's actions, such as registry changes, file access, network activity, and creates reports that help to understand how the programme interacts with the system.

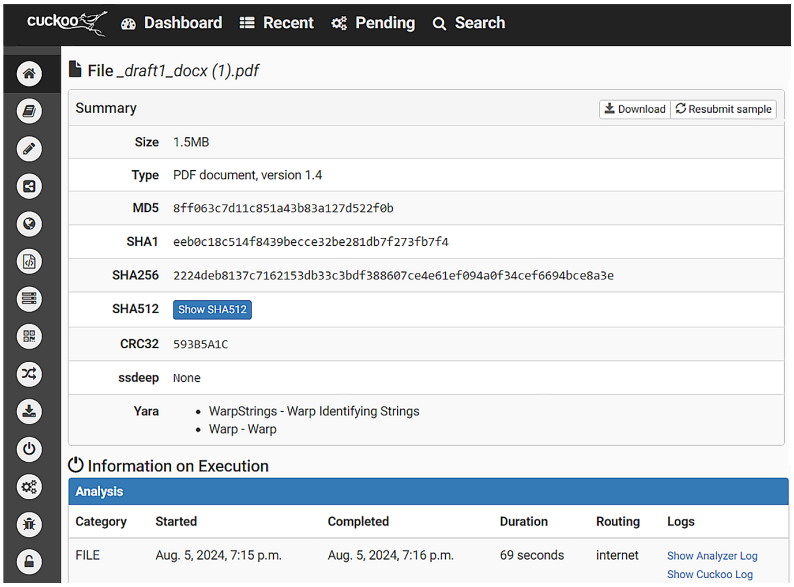

Figure 5. Example of using Cuckoo Sandbox to check file security
Source: compiled by the author

The Figure 5 illustrates how Cuckoo Sandbox creates an isolated environment for malware execution, tracks its behaviour, and collects data for further analysis. In addition to these tools, there are many other platforms that specialise in detecting malware. For example, Snort is an open-source intrusion detection system that monitors network traffic and analyses it for malicious activity. It detects abnormal behaviour, analyses packets, and monitors traffic. Suricata is a powerful open-source IDS/Intrusion Prevention System (IPS) that supports deep packet analysis and network monitoring. Its functions include checking network traffic, analysing threats, recognising protocols, and blocking attacks. There is also Malwarebytes, an antivirus and antispyware tool that specialises in detecting and removing malicious software and spyware, viruses, trojans, and adware. Yara is a tool for creating and using templates to detect and classify malicious files. It detects and analyses malicious patterns using templates and threat recognition. In turn, Hybrid Analysis is an online platform for dynamic and static malware analysis. It analyses file behaviour, collects information about requests, system changes, and network activity. ReversingLabs offers malware analysis platforms that include tools for static and dynamic analysis. This tool conducts research of malicious samples, detection of threats, and tracking the origin of malicious software. In addition, there are tools such as FireEye, OpenDXL, Threat Grid, SIEM systems, SOAR platforms, and EDR solutions. These tools and platforms play a key role in cybersecurity, helping organisations to effectively detect, analyse, and respond to malware and cyber threats.

In general, the development of malicious software encourages continuous progress in security systems and new cybersecurity technologies. With the growing complexity and diversity of cyber threats, cybersecurity professionals are forced to develop new solutions to detect and counter these threats. Modern security methods include innovative approaches and technologies that evolve in response to the emergence of new types of malwares. Antivirus programmes are among the oldest tools in the fight against malicious software. Modern antivirus systems use a combination of traditional signature techniques and more modern technologies, such as machine learning and behavioral analysis. Signature methods are based on recognising known malware patterns, while behavioural analysis detects new or unknown threats based on their activity in the system. These programmes include CCleaner (Fig. 6). CCleaner, although not an antivirus, is a popular tool for cleaning the system of temporary files, cache, and other unnecessary data. It helps to improve overall system performance and remove potentially unwanted applications. While CCleaner does not provide specific malware protection directly, using it can help to keep system clean and reduce the chance of infection.

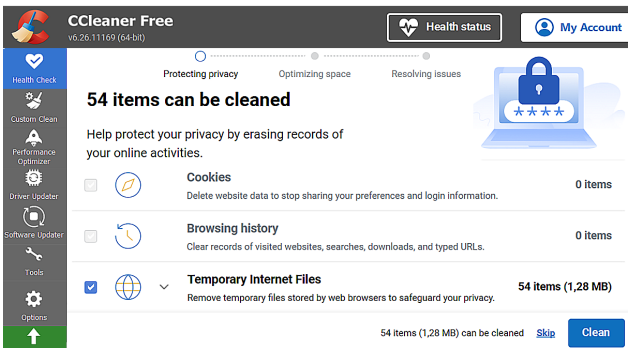

Figure 6. Example of using CCleaner utility software
Source: compiled by the author

Attention should also be paid to Norton Antivirus, which is one of the most well-known antivirus solutions. It provides a high level of protection due to powerful signature databases and behavioural analysis. Norton has effective features for detecting and blocking malicious software and spam mailings. However, its resource intensity can affect the speed of the system, and there are also constant updates that can be intrusive for users. The strong point of Bitdefender is its security technology and low impact on system performance. This application uses innovative security techniques such as machine learning and anti-phishing to ensure a high level of security. Bitdefender also offers features to protect sensitive data and ensure online activity. This solution is marked by a good balance between powerful protection and low resource consumption. In turn, McAfee offers comprehensive protection that includes not only antivirus features, but also protection against malicious websites and real-time threats. Its security mechanisms are robust, but sometimes McAfee can be noticeable in the system and consume a significant number of resources. In addition, Avast offers a free version with basic protection, including paid versions with advanced features. It performs well in virus detection and has a user-friendly interface. Avast provides privacy protection and blocking unwanted programmes. Thus, Norton Antivirus provides a high level of protection, but can be somewhat resource-intensive and have privacy issues. Bitdefender offers a balanced approach with powerful protection and low resource consumption. McAfee has comprehensive protection, but can consume a significant amount of system resources. Avast offers a user-friendly interface and a free version, but sometimes it can affect the system speed. And CCleaner is useful for maintaining overall system performance, but it does not replace specialised anti-malware solutions. However, Norton, TotalAV, McAfee, Intego, Bitdefender, Malwarebytes, and Panda are considered the best antivirus programmes of 2024 (Fig. 7).

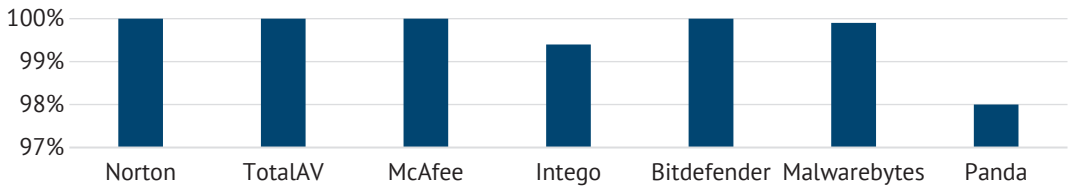

Figure 7. Rating of antivirus programmes in 2024

Source: compiled by the author

As for intrusion detection systems, they monitor network traffic and system activity to detect abnormal behaviour that may indicate an attack attempt (Fig. 8). IDS can be either signature-based or anomaly-based. Signature-based systems compare traffic to known attack patterns, while anomaly-based systems detect deviations from normal behaviour that may indicate new threats. There are systems such as OSSEC, Zeek, Security Onion.

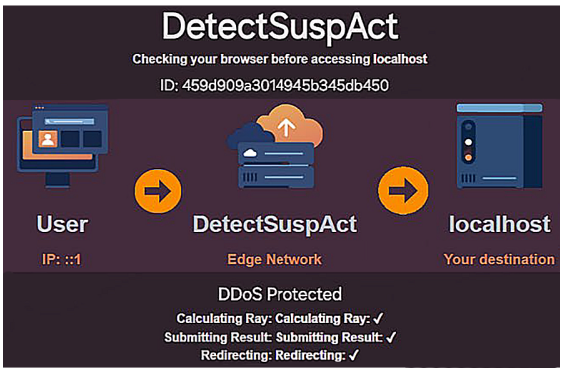

Figure 8. Example of using IDS

Source: A. Tsymbal (2024)

Firewalls are also important, which monitor incoming and outgoing network traffic based on a set of security rules and policies. Modern firewalls include deep packet analysis features that allow detecting malicious traffic and blocking it before it reaches end devices. They can be either hardware or software and provide multi-level protection. Examples include Cisco ASA, Palo Alto Networks Next-Generation Firewall, Check Point Firewall, and Sophos XG Firewall. An important aspect of cybersecurity is the education of users. Training users in the basics of cybersecurity, such as detecting phishing emails, and recognising malicious attachments, is critical to reducing the risk of malicious software infecting the system. Educational programmes often include security training and attack simulations to help users raise their awareness and readiness for cyber threats.

Regarding the effectiveness of modern protection methods, several key aspects have been identified. First, the combination of antivirus programmes, IDS, firewalls, and user education provides multi-level protection, which is important for reducing risks. Secondly, modern security systems are constantly being improved to deal with new types of malicious software. Machine learning and behaviour analysis technologies play a key role in identifying new threats. Thirdly, enabling proactive methods, such as regular software updates and system patches, helps to reduce vulnerabilities that can be exploited by attackers. Thus, anti-malware

methods are constantly evolving in response to new cyber threats. The integration of various approaches and technologies, together with user education, provides comprehensive protection against malware and reduces the risks of cyber threats.

DISCUSSION

The study showed the importance of implementing integrated security systems in modern networks, where the integration of the latest security technologies plays a key role in ensuring data integrity and confidentiality. Analysis of the findings in the context of existing studies indicates the importance of a systematic approach to the problem of cybersecurity, in particular, in the context of new threats and security technologies. The importance of such an analysis lies in the fact that it allows identifying new trends and approaches in the field of information security and supporting practical recommendations based on the results of previous research. This contributes to the further development and improvement of security methods, which is critical in the rapidly changing cyber environment.

The results of this study showed that the integration of the latest cryptographic algorithms and security technologies significantly improves the level of information protection. This correlates with the findings of W. Stallings & L. Brown (2018), who examined current cybersecurity principles, including cryptographic algorithms and general security principles. Their study confirmed the importance of implementing effective cryptography methods to ensure data security, which is consistent with the results obtained, which focuses on improving existing security methods through the latest cryptographic solutions. Meanwhile, M. Bishop (2018) addressed a wide range of issues related to modern security techniques, including attack analysis and intrusion detection. This study also confirmed that the integration of new security technologies increases the effectiveness of intrusion detection systems and reduces the risks that can arise from modern attacks. This highlights the importance of constantly updating and adapting security methods in the face of new threats, as shown in this paper, where the emphasis was placed on the latest methods of ensuring system security.

The study noted an increase in the complexity of modern attacks and malware, which requires advanced protection measures. In turn, the J. Ferdous *et al.* (2023) confirmed that the integration of multi-layer security systems can effectively counteract new types of threats, such as cryptojacking and attacks on IoT devices. In addition, this study is consistent with the conclusions of M. Jartelius (2020), who emphasised the importance of a proactive approach to threat detection to prevent data leaks, confirming the effectiveness of the integrated security systems implemented in this paper. The results of the study also indicate the importance of implementing innovative methods in the field of cybersecurity, such as automation and the use of the latest machine learning algorithms. This correlates with the findings of M. Conti *et al.* (2018), considered the security issues in IoT, and with the results of the study by Z. Chen (2020), where modern deep learning algorithms for malware protection were investigated. This study confirmed that the use of the latest technologies, such as deep learning, can significantly improve the effectiveness of protection systems against new types of cyber threats. In addition, the results of this study, which highlighted the effectiveness of post-quantum cryptography in data protection, are consistent with the study by P.N. Kokare *et al.* (2024), which compares traditional cryptography with post-quantum algorithms. Also important is the contribution of I. Legárd (2020), which focused on raising staff awareness of information security, which is critical to maintaining a high level of protection. This study has confirmed that an effective awareness-raising programme can have a significant impact on reducing the risks of cyber threats.

The results showed that the effectiveness of data protection can be improved by using the latest machine learning algorithms and automated systems. This is consistent with the conclusions of N. Akhter *et al.* (2021), who described how hackers exploited vulnerability in SolarWinds Orion software suite to compromise systems. They emphasised that timely detection and elimination of such vulnerabilities is crucial to prevent large-scale data leaks. In addition, the results of this study, which emphasised the importance of integrating multi-layer security systems to prevent attacks, correlate with the study by T. Olaniyan (2021), who also described the hacking of FireEye through the SolarWinds Orion update platform. The analysis showed that an attack on such a platform can lead to significant consequences for the security of organisations, which emphasises the need for comprehensive protection and rapid response to threats. Moreover, the results of this study showed the importance of continuously implementing the latest machine learning techniques in cybersecurity. T. Khatun (2024) also reviewed malware development and strategies in detail, which is consistent with the results of this study, which focused on the evolution of malware and the need to improve detection methods. This highlights the importance of continuous monitoring and adaptation to new threats.

It is worth noting that the results of this study focus on the evolution of malware and methods of combating it, which has common aspects with the papers by S. Okhanashvili (2023). The paper highlighted the importance of an integrated approach to improving cybersecurity, considering technical, programme, and organisational aspects. This study also confirms the importance of a comprehensive approach in the fight against cyber threats, but focuses on the evolution of malicious software and changes in its complexity over time. In addition, the results obtained share common features with the studies by K.K. Dewangan *et al.* (2024) and N.S. Janoti *et al.* (2024). In the first case,

the researchers investigated cyber threats to intelligent transport systems, focusing on new technologies such as blockchain and 5G to improve security. The current study also explored innovative approaches to security, but with an emphasis on general trends in the evolution of malicious software. In the second case, the researchers considered challenges in Cyber Threat Intelligence and the role of data analysis in protecting against cyber threats. The results also focused on the importance of data to combat evolutionary threats, but focused more on changes in the malware itself and its impact on cybersecurity. Ultimately, the study by O.C. Obi *et al.* (2024) also shares similarities with this study, as it offered a comprehensive overview of the current cybersecurity landscape, focusing on various threats such as malware and advanced persistent threats. However, the current study confirmed this trend, in particular in the context of the evolution of malware. Overall, the conducted study confirms the findings of other researchers on the evolution of malware and highlights the importance of comprehensive strategies to combat modern cyber threats. This is important for developing more effective strategies to protect against cyber threats in the future.

CONCLUSIONS

A study of the evolution of malicious software has confirmed that the development of malicious software has gone through several key stages, from simple viruses to modern complex cyber threats, such as ransomware and spyware. This study highlighted how changes in attack technologies and tactics lead to a constant increase in complexity and potential malware damage. Analysis of modern threats has shown that malicious software actively uses advanced technologies, including artificial intelligence, to bypass security systems. This creates new cybersecurity challenges that require organisations to implement more comprehensive and dynamic security strategies. Regular software updates, the introduction of intrusion detection systems, and the continuous improvement of cybersecurity tools are critical to countering modern threats. This study also highlighted the growing use of new attack methods, such as phishing and business email hacking. These new methods require organisations to implement additional security measures, such as multi-factor authentication and regular employee training. The use of advanced tools to analyse and monitor network traffic is also critical for early detection of suspicious activity. The importance of collaboration between different organisations and cybersecurity professionals is a key to improving security. Sharing of information about new threats and vulnerabilities, joint development of security methods and educational programmes can significantly improve the effectiveness of cybersecurity.

The main recommendations for improving cybersecurity include the introduction of regular updates of systems and software, the use of modern detection and prevention tools, the development of comprehensive protection strategies covering technical and organisational measures, and active cooperation with other experts in the field of cybersecurity. However, the study has some limitations, including a limited number of specific cases for analysing the evolution of malware and the complexity of assessing the impact of the latest technologies on all aspects of cybersecurity. Further research may include a more detailed analysis of new types of attacks, emerging technologies, and an assessment of their impact on various industries and sectors.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Akhter, N., Aziz, O., & Hussain, T. (2021). Latest trends in the cybersecurity after the solar wind hacking attack. *Foundation University Journal of Engineering and Applied Sciences*, 1(2). doi: 10.33897/fujeas.v1i2.347.

[2] Alchi, A., Dodiya, K., & Niveditha, V.S. (2024). Impact of neural network on malware detection. In K. Kaushik & I. Sharma (Eds.), *Next-generation cybersecurity* (pp. 219-241). Singapore: Springer. doi: 10.1007/978-981-97-1249-6_10.

[3] Anderson, R.J. (2020). *Security engineering: A guide to building dependable distributed systems*. London: Wiley. doi: 10.1002/9781119644682.

[4] Antonenko, N., Dihtyar, Ya., & Krykun, N. (2022). Modern methods of fighting computer viruses. *Economy and Society*, 43. doi: 10.32782/2524-0072/2022-43-51.

[5] Bishop, M. (2018). *Computer security: Art and science*. Boston: Addison-Wesley.

[6] Chen, Z. (2020). Deep learning for cybersecurity: A review. In *International conference on computing and data science* (pp. 7-18). Stanford: IEEE. doi: 10.1109/CDS49703.2020.00009.

[7] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78(2), 544-546. doi: 10.1016/j.future.2017.07.060.

[8] Dalman, J., & Smith, H. (2021). *Under attack: Protecting against Conti, DarkSide, REvil and other ransomware*. Retrieved from https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/.

[9] Dewangan, K.K., Panda, V., Ojha, S., Shahapure, A., & Jahagirdar, S.R. (2024). Cyber threats and its mitigation to intelligent transportation system. In *Symposium on international automotive technology*. Warrendale, Pennsylvania: SAE International. doi: 10.4271/2024-26-0184.
[10] Durmuş Şenyapar, H.N. (2024). Digital marketing in the age of cyber threats: A comprehensive guide to cybersecurity practices. *The Journal of Social Science*, 8(15), 1-10. doi: 10.30520/tjsosci.1412062.
[11] Ferdous, J., Islam, R., Mahboubi, A., & Islam, M.Z. (2023). A review of state-of-the-art malware attack trends and defense mechanisms. *IEEE Access*, 11, 121118-121141. doi: 10.1109/ACCESS.2023.3328351.
[12] Galuzin, I., & Naiman, G. (2021). Vulnerability management of corporate information systems based on QUALYS solutions. *Modern Information Security*, 46(2), 26-31. doi: 10.31673/2409-7292.2021.020708.
[13] Hanna, K.T. (2021). *Chernobyl virus*. Retrieved from https://www.techtarget.com/searchsecurity/definition/Chernobyl-virus.
[14] Janoti, N.S., Rohan, Rida, & Negi, N. (2024). Strategic perspectives on cyber threat intelligence: A comprehensive analysis. *International Journal for Research in Applied Science and Engineering Technology*, 12(4), 524-529. doi: 10.22214/ijraset.2024.59816.
[15] Jartelius, M. (2020). The 2020 data breach investigations report – a CSO's perspective. *Network Security*, 2020(7). doi: 10.1016/S1353-4858(20)30079-9.
[16] Karlberg, L.A. (2004). *Sasser faster than Blaster*. Retrieved from https://www.nyteknik.se/nyheter/sasser-snabbare-an-blaster/425179.
[17] Khatun, T. (2024). *Malware – unmasking the pervasive cyber threat of 2023*. Retrieved from https://www.researchgate.net/publication/382442937_Malware-_Unmasking_the_Pervasive_Cyber_Threat_of_2023.
[18] Kokare, P.N., Vora, D., Patil, S., Kotecha, K., Khairnar, V., Choudhury, T., & Kulkarni, A. (2024). *Post quantum cryptography: A survey of past and future*. Retrieved from https://www.researchgate.net/publication/382398375_Post_Quantum_Cryptography_A_survey_of_Past_and_Future.
[19] Kumar, S., & Nagar, G. (2024). Threat modeling for cyber warfare against less cyber-dependent adversaries. *Proceedings of the 23rd European Conference on Cyber Warfare and Security*, 21(1), 257-264. doi: 10.34190/eccws.23.1.2462.
[20] Legárd, I. (2020). Building an effective information security awareness program. *Central and Eastern European eDem and eGov Days*, 338, 189-200. doi: 10.24989/ocg.338.15.
[21] Marchenko, O. (2023). Cybersecurity and information protection: Analysis of the impact of risks and threats using modern effective cyberspace protection strategies. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 50-59. doi: 10.32782/IT/2023-3-6.
[22] Matthews, T. (2022). *Creeper: The world's first computer virus*. Retrieved from https://www.exabeam.com/blog/infosec-trends/creeper-the-worlds-first-computer-virus/.
[23] Nemchick, E. (2023). *What is Pegasus spyware+how to remove it from your mobile device?* Retrieved from https://us.norton.com/blog/emerging-threats/pegasus-spyware.
[24] Obi, O.C., Akagha, O.V., Dawodu, S.O., Anyanwu, A.C., Onwusinkwue, S., & Ahmad, I.A.I. (2024). Comprehensive review on cybersecurity: Modern threats and advanced defense strategies. *Computer Science & IT Research Journal*, 5(2), 293-310. doi: 10.51594/csitrj.v5i2.758.
[25] Okhanashvili, S. (2023). Cyber security and malware. *"Intercultural Dialogues" Transactions*, 7. doi: 10.52340/idw.2023.72.
[26] Olaniyan, T. (2021). *Applying the diamond model of intrusion analysis: FireEye breach*. Retrieved from https://www.researchgate.net/publication/354254596_Applying_the_Diamond_Model_of_Intrusion_Analysis_FireEye_Breach.
[27] Qumer, M., & Ikrama, S. (2022). Poppy Gustafsson: Redefining cybersecurity through AI. *The Case for Women*, 1-38. doi: 10.1108/CFW.2022.000001.
[28] Ravi, P., Bhargav, K.S., Venkatesh, P.M.M., Princy, M., & Reddy, M.R. (2024). Empowering security with machine learning for ransomware and malware detection. *International Journal of Scientific Research in Engineering and Management*, 8(4), 1-5. doi: 10.55041/IJSREM30675.
[29] Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice*. London: Pearson.
[30] Tsymbal, A. (2024). *Development of a system for detecting suspicious activities in computer networks*. (Bachelor's thesis, Black Sea National University named after Petro Mohyla, Mykolaiv, Ukraine).
[31] Zulkovska, I., Pluzhnik, A., & Zhulkovski, O. (2021). Modern methods of detection of malware. *Mathematical Modelling*, 44(1), 46-54. doi: 10.31319/2519-8106.1(44)2021.235922.

Розробка шкідливих програм: від ранніх вірусів до сучасних кіберзагроз

Денис Ковальчук
Аспірант
Міжнародний гуманітарний університет
65009, дор. Фонтанська, 33, м. Одеса, Україна
https://orcid.org/0009-0003-2302-8698

Анотація. Шкідливі програми є однією з найбільших загроз у цифровому середовищі, оскільки вони постійно еволюціонують і стають все більш небезпечними. Метою цього дослідження був аналіз еволюції зловмисного програмного забезпечення. Для досягнення цієї мети було застосовано історичний, порівняльний та емпіричний аналіз, а також оцінка існуючих захисних технологій. Основні результати дослідження виявили кілька ключових етапів розвитку шкідливих програм. Історичний аналіз показав, що еволюція шкідливих програм пройшла через кілька значних стадій, від простих вірусів і черв'яків до складних загроз, таких як програми-вимагачі і шпигунські програми. Ці зміни були зумовлені технологічними досягненнями і розширенням можливостей для атак, що дозволило шкідливому програмному забезпеченню використовувати нові вектори впливу та методи обману. Порівняльний аналіз сучасних кіберзагроз розкрив ключові характеристики та відмінності між різними типами шкідливих програм, а також їхні специфічні методи розповсюдження і вразливості. Виявлено, що нові загрози мають складнішу архітектуру і використовують більш інноваційні тактики, що значно ускладнює їхнє виявлення та нейтралізацію. Емпіричний аналіз, що включав використання інструментів виявлення загроз, надав конкретні дані про поведінку шкідливих програм у реальних умовах. Огляд і тестування сучасних методів захисту, включаючи антивірусні рішення, системи виявлення вторгнень та міжмережеві екрани, показали їхні сильні та слабкі сторони, а також їх ефективність у виявленні і запобіганні новим загрозам. Результати дослідження підкреслили необхідність постійного вдосконалення методів захисту, що є критично важливим для ефективної боротьби з сучасними кіберзагрозами

Ключові слова: еволюція інформаційних атак; цифрова безпека; системи виявлення вторгнень; захисні технології; аналіз комп'ютерних інцидентів