АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР
ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ
INFORMATION AND COMMUNICATION TECHNOLOGIES

АҚПАРАТТЫҚ ҚАУІПСІЗДІК
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
INFORMATION SECURITY

DOI 10.51885/1561-4212_2025_1_138
IRSTI 81.93.29

D.M. Zhaksibek[1], Zh.Zh. Akhmetova[1], P. Popov[2], B.A. Serimbetov[3]
[1]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
E-mail: zhaksibek.dias@icloud.com
*E-mail: zaigura@mail.ru**
[2]City University London, London, UK
E-mail: p.t.popov@city.ac.uk
[3]Kazakh University of Technology and Business named after K. Kulazhanov,
Astana, Kazakhstan
E-mail: sba_rnmc@mail.ru

COMPARATIVE ANALYSIS OF RANSOMWARE DECRYPTION METHODS

БОПСАЛАУШЫ-БАҒДАРЛАМАНЫҢ ШИФРЫН ШЕШУ ӘДІСТЕРІНІҢ САЛЫСТЫРМАЛЫ ТАЛДАУЫ

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ДЕШИФРОВАНИЯ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Abstract. *Ransomware is one of the most serious cybersecurity threats, as it can have a devastating impact on private users, businesses and government agencies alike. This survey paper analyses current ransomware decryption techniques, which include approaches such as brute-force, vulnerability analysis, specialised decryptors and machine learning techniques. The aim of the study is to provide a comprehensive analysis of existing methods to determine their effectiveness, resource costs and limitations.*

Particular attention is given to methods utilising artificial intelligence due to their significant potential in improving decryption efficiency and developing adaptive solutions. The analysis shows that machine learning and AI can significantly accelerate vulnerability detection and improve decryption accuracy. The results of the study highlight the importance of leveraging these advanced technologies to better protect systems from threats posed by ransomware.

The practical relevance of the paper is that it provides cybersecurity professionals with valuable insights into the selection of appropriate defence techniques and possible ways to improve them. The article also reveals directions for future research, focusing on the need to develop more versatile and effective defence tools. The authors demonstrate that integrating new technologies into existing approaches can significantly reduce risks and increase the resilience of systems. Thus, the presented material contributes to the knowledge and understanding of modern decryption techniques and their role in combating ransomware, making it an important contribution to the development of the industry.

Keywords: *Ransomware, encryption, decryption, artificial intelligence, machine learning.*

Аңдатпа. *Бопсалаушы-программалар киберқауіпсіздік саласындағы ең үлкен қауіптердің бірі болып табылады, өйткені олар жеке пайдаланушыларға, кәсіпорындарға және мемлекеттік мекемелерге айтарлықтай зиян келтіруі мүмкін. Осы шолу мақаласы бопсалаушы-программаларды дешифрлаудың заманауи әдістерін талдауға арналған, оған парольдерді таңдау (brute-force), осалдықтарды талдау, арнайы дешифраторларды пайдалану және машиналық оқыту технологияларын қолдану сияқты әдістер кіреді.*

Зерттеудің мақсаты – қолданыстағы әдістерді олардың тиімділігін, ресурстар шығындарын *және шектеулерін анықтау үшін жан-жақты талдау.*

Жасанды интеллектті қолданатын әдістерге ерекше назар аударылады, себебі олардың дешифрлау тиімділігін арттыруда және бейімделгіш шешімдерді жасауда айтарлықтай әлеуеті бар. Талдау машиналық оқыту мен ЖИ осалдықтарды анықтау үдерісін едәуір жеделдетіп, дешифрлау дәлдігін арттыра алатынын көрсетеді. Зерттеудің нәтижелері бұл озық технологияларды жүйелерді бопсалаушы-программалардан туындайтын қауіптерден қорғауды жақсарту үшін пайдаланудың маңыздылығын айқындайды.

Мақаланың практикалық маңыздылығы – ол киберқауіпсіздік саласындағы мамандарға қорғау әдістерін таңдау және оларды жетілдіру жолдары туралы құнды мәліметтер береді. Мақала сондай-ақ болашақ зерттеулерге бағыттар көрсетіп, әмбебап және тиімді құралдарды әзірлеу қажеттілігіне назар аударады. Авторлар жаңа технологияларды қолданыстағы әдістерге біріктіру жүйелердің тәуекелдерін айтарлықтай төмендетіп, олардың тұрақтылығын арттыра алатынын дәлелдейді. Осылайша, ұсынылған материал бопсалаушы-программалармен күресте қазіргі дешифрлау әдістерінің рөлі мен маңыздылығын түсінуді тереңдетуге ықпал етеді, бұл оны саланың дамуына маңызды үлес етеді.

Түйін сөздер: *Бопсалаушы-программалар, шифрлау, дешифрлау, жасанды интеллект, машиналық оқыту.*

Аннотация. *Программы-вымогатели представляют одну из самых серьезных угроз в области кибербезопасности, поскольку они могут нанести разрушительное воздействие как на частных пользователей, так и на предприятия и государственные учреждения. Данная обзорная статья посвящена анализу современных методов дешифрования программ-вымогателей, которые включают такие подходы, как перебор паролей (brute-force), анализ уязвимостей, применение специализированных дешифраторов и использование технологий машинного обучения. Целью исследования является предоставление всестороннего анализа существующих методов для определения их эффективности, затрат ресурсов и ограничений.*

Особое внимание уделено методам, использующим искусственный интеллект, благодаря их значительному потенциалу в повышении эффективности дешифрования и разработке адаптивных решений. Анализ показывает, что машинное обучение и ИИ могут существенно ускорить процесс выявления уязвимостей и повысить точность дешифровки. Результаты исследования подчеркивают важность использования этих передовых технологий для повышения защиты систем от угроз, исходящих от программ-вымогателей.

Практическая значимость статьи заключается в том, что она предоставляет специалистам в области кибербезопасности ценные сведения о выборе подходящих методов защиты и возможных путях их совершенствования. Статья также раскрывает направления для будущих исследований, акцентируя внимание на необходимости разработки более универсальных и эффективных инструментов защиты. Авторы демонстрируют, что интеграция новых технологий в существующие подходы способна значительно снизить риски и повысить устойчивость систем. Таким образом, представленный материал способствует углублению знаний и пониманию современных методов дешифрования и их роли в борьбе с программами-вымогателями, что делает его важным вкладом в развитие отрасли.

Ключевые слова: *Программы-вымогатели, шифрование, дешифрование, искусственный интеллект, машинннное обучение.*

Introduction. Ransomware is a type of malicious software that encrypts user data, making it inaccessible, and demands a ransom for its restoration. In recent years, it has become one of the most serious and widespread cyber threats, causing significant damage to individuals and organizations of various scales.

The consequences of ransomware attacks go beyond the financial losses associated with ransom payments. Victims face business process disruptions, loss of critical data, and reputational damage, which can have long-term negative effects (Shaukat, S. & Ribeiro B., 2020).

Literature review. The relevance of research into ransomware decryption techniques stems from the growing threat of ransomware to users and organisations around the world. The number of ransomware incidents increases every year, and the consequences of such attacks can be catastrophic, including loss of confidential data, financial losses and reputational risks. The difficulty of decrypting such programs is caused by the use of complex cryptographic algorithms, which requires the development of new methods and technologies to analyse them (Ahmad, A., Webb, J., Desouza, K. C., & Boorman J.,2019).

Despite active research in the field of ransomware decryption, there are a number of shortcomings in methodologies and research gaps (Retrieved from https://www.cisa.gov/ransomware):

– Limitations of universal solutions. One of the main drawbacks of existing methods is their limited applicability to different types of ransomware. Each new virus may use unique ciphers and defence mechanisms, making it difficult to create universal decryption tools.

– Lack of open data. Many decryption methods depend on public repositories that store encryption keys. However, these repositories are not always complete, and many cybercriminals use methods that leave no trace for later analysis.

– Lack of a comprehensive approach. Research often focuses on narrow aspects of decryption (e.g. decrypting one particular virus), but does not always consider the need for a comprehensive approach that includes both technical and organisational security measures to prevent attacks.

– Problems with machine learning. Although machine learning techniques are advancing in the analysis of ransomware, these techniques have limited effectiveness because many programs use dynamic encryption techniques and also attempt to hide their actions from analysis (Retrieved from https://www.europol.europa.eu/media-press/newsroom/news/no-more-ransom-celebrates-five-years-of-stopping-ransomware).

Materials and methods of research. To understand how an attacker (such as the author of a ransomware) uses symmetric and asymmetric encryption, we need to look at a typical ransomware scheme and the ways in which they block access to data by demanding a ransom (Figure 1).

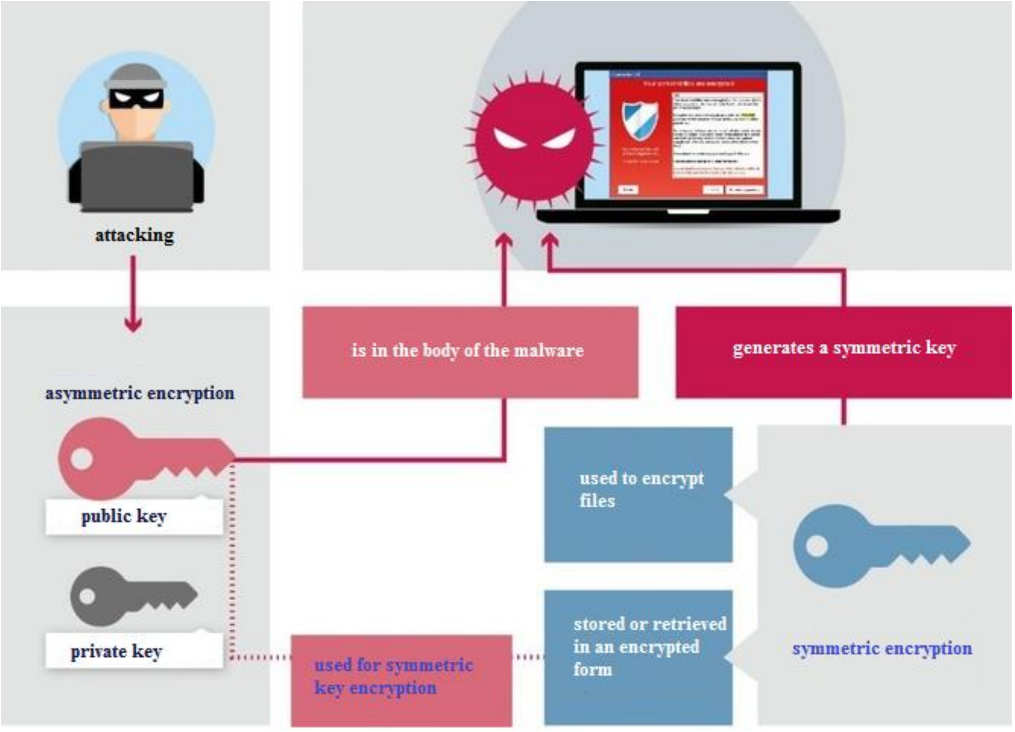
attacking
asymmetric encryption
public key
private key
is in the body of the malware
generates a symmetric key
used to encrypt files
stored or retrieved in an encrypted form
used for symmetric key encryption
symmetric encryption

Figure 1. A schematic of how symmetric and asymmetric encryption works, which is used in encryptors (Note – compiled by the authors on the basis of the source: https://www.trendmicro.com/ru_ru/what-is/ransomware.html)

Typically, ransomware combines two types of encryption to achieve its goal: symmetric (to encrypt data) and asymmetric (to protect the decryption key) (Mora S., Bongiovanni G., Giacinto G., & Perdisci R., 2020).

1. Introduction and initial phase of the attack

Malware distribution: The attacker injects the encryptor onto the victim's device via phishing emails, malicious links, software vulnerabilities, or remote access.

Initial launch phase: After infiltration, the encryptor begins scanning the victim's system for data that can be encrypted and selects files based on a predefined algorithm (Al-Rimy B.A.S., Maarof M.A., & Shaid S.Z. M., 2018).

2. Generating a symmetric key to encrypt the data

Symmetric key generation: A random symmetric key (e.g. for AES encryption) is created on the victim's device. This key will be used to encrypt all data.

Data encryption using symmetric key: The encryptor applies a symmetric key to quickly encrypt all detected files. Symmetric encryption (e.g. AES) is used because of its speed and efficiency in encrypting large amounts of data (Azmoodeh, A., Dehghantanha, A., Choo, K. K. R., & Conti, M., 2018).

3. Using asymmetric encryption to protect the symmetric key

Symmetric key encryption: Once the data is encrypted, the symmetric key itself becomes critical for file recovery. The attacker uses asymmetric encryption (e.g. RSA) to encrypt the symmetric key. The RSA public key used to encrypt the symmetric key is pre-embedded in the malware code and known only to the attacker (Li, Y., & Guo, L., 2019).

Removing the symmetric key from memory: Once the symmetric key is encrypted and stored in encrypted form, the original unencrypted key is removed from the memory of the victim's system. This makes it impossible to decrypt the data without accessing the attacker's private key, which is stored on the attacker's side.

4. Ransom notice and demand

Creating a ransom message: The encryptor displays a ransom message to the victim stating that her files are encrypted and a private key is required to regain access. This message usually includes instructions on how to pay the ransom (e.g., in cryptocurrency) and possible ways to contact the attacker (Retrieved from https://www.nomoreransom.org.).

Promise of decryption: The attacker states that after receiving payment, he will provide a private key or decrypter that will allow the files to be recovered. This key is needed to decrypt the encrypted symmetric key and then, using the symmetric key, return the data to its original state.

5. Decryption (after paying the ransom)

If the victim agrees to the terms and pays the ransom, the attacker can provide the victim with the private key or a special decryption software (Asghar M.R., Habib S., & Javed M.Y., 2020). In this case:

Symmetric key decryption: First, the victim uses the provided private key to decrypt the symmetric key.

Data decryption: The symmetric key is then used to decrypt the encrypted data, restoring it to its original state.

Reasons for choosing a combination of symmetric and asymmetric encryption

Speed and efficiency: Symmetric encryption such as AES is much faster, allowing large amounts of data to be encrypted in a short period of time.

Key Security: Asymmetric encryption protects the symmetric key because the private key to decrypt it is stored with the attacker. This minimises the risk of the victim being able to obtain the symmetric key without ransom.

This combined scheme of working with symmetric and asymmetric encryption allows the encryptor to achieve maximum efficiency and security. The victim cannot decrypt his data without access to the private key, which is controlled by the attacker, and at the same time the encryption process is fast due to the use of the symmetric key (Shaukat S., & Ribeiro B., 2018).

Therefore, the development of effective methods for ransomware decryption is becoming increasingly important. The ability to restore access to encrypted data without paying the ransom reduces the motivation of attackers and helps decrease the prevalence of such attacks (Vinayakumar, R., et al., 2019).

The purpose of this article is to conduct a comparative analysis of various ransomware decryption methods, identify their advantages and limitations, and discuss the prospects for using artificial intelligence to enhance the effectiveness of these methods.

Results and their discussion

Approaches to Ransomware Decryption:

1.Brute-force Method. The brute-force method is based on systematically trying all possible decryption key combinations until the correct one is found (Sgandurra D., & Lupu E. C., 2016). This approach, while straightforward, is extremely resource-intensive and time-consuming. Its effectiveness heavily depends on the complexity of the encryption algorithm used (Figure 2).

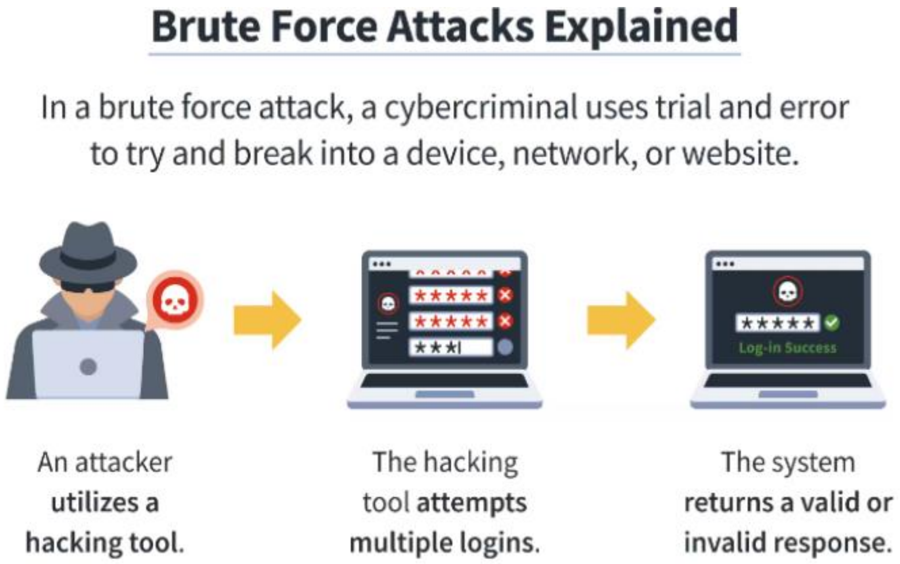
Brute Force Attacks Explained
In a brute force attack, a cybercriminal uses trial and error to try and break into a device, network, or website.
Log-in Success
An attacker utilizes a hacking tool.
The hacking tool attempts multiple logins.
The system returns a valid or invalid response.

Figure 2. Brute-force attacks explained
*(*Note – compiled by the authors on the basis of the source: *https://www.xcitium.com/brute-force-attacks/)*

The advantages of the brute-force method lie in its simplicity and universality. It can be effective when simple encryption algorithms are used, as it does not require deep knowledge of the software itself. This makes it a useful tool for the initial stage of analysis and decryption.

However, despite its simplicity and universality, the brute-force method has significant limitations. It is highly resource-intensive and can take a considerable amount of time, especially when dealing with long keys or complex encryption algorithms. This makes it impractical for real-world scenarios where quick data recovery is essential. Moreover, the brute-force method is ineffective against complex encryption algorithms used in modern ransomware (Huang J., Xu Z., Chen Y., & Tang H., 2020). In such cases, trying all possible combinations becomes virtually impossible due to the vast number of key options.

Advantages:

Direct method: Works for any encrypted data where the key is unknown, especially if the encryption algorithm is uncomplicated and the key is short.

Automation: Can be implemented through scripts and programs, making the task easier for the user.

Limitations:

High time cost: Password brute force requires significant time, especially for long keys and modern encryption algorithms (e.g., AES-256).

Computational resources: For complex keys, the method becomes inefficient and requires large computational power.

2. Vulnerability Analysis. Vulnerability analysis focuses on identifying weaknesses in the ransomware implementation that allow bypassing the encryption or obtaining the decryption keys (Laszka A., Farhang S., & Grossklags J., 2017). Instead of attempting to crack the encryption code directly, as in brute-force methods, vulnerability analysis looks for weaknesses in the ransomware's implementation. For example, some ransomware may use weak or predictable algorithms for key generation, making them susceptible to attacks. In other cases, the decryption key might be stored in memory or on disk in an unencrypted form, making it possible to extract.

Security experts use various techniques for vulnerability analysis, such as reverse engineering, dynamic analysis, and static analysis (Cabaj K., Kotulski Z., Mazurczyk W., & Mazurczyk W., 2018). When a vulnerability is discovered, it can be exploited to bypass the encryption or retrieve the decryption key. Vulnerability analysis can be effective against a wide range of ransomware, including those using complex encryption algorithms. Finding vulnerabilities can lead to the development of universal decryption solutions that can be used against different types of ransomware.

However, vulnerability analysis requires deep knowledge of ransomware, encryption methods, and reverse engineering skills. Finding and exploiting vulnerabilities can be a time-consuming process, especially for new or unknown ransomware variants. Additionally, vulnerabilities may be patched in new versions of ransomware, reducing this method's effectiveness.

Despite these limitations, vulnerability analysis remains one of the most effective ransomware decryption methods.

Advantages:

High efficiency: If a vulnerability is present, decryption can be performed quickly and without computational cost.

Targeted approach: This method can be effective for specific ransomware that has bugs.

Limitations:

Limited application: Vulnerabilities are not always present, and this method is only applicable to specific versions of encryption ransomware.

Difficulty of finding: Requires reverse-engineering and code analysis skills to find bugs, which can be time-consuming.

3. Use of Expert-Created Decryptors. Cybersecurity experts develop specialized decryption tools based on a detailed analysis of specific ransomware (Kolodenker E., Koch W., Stringhini G., & Egele M., 2017). Creating a decryptor typically involves analyzing the ransomware, developing the decryption algorithm, and building the decryption tool. Expert-created decryptors can be very effective for specific ransomware variants for which they were developed. In some cases, they can decrypt files without needing the decryption key. Many decryptors are available for free or at a low cost.

However, a decryptor created for one ransomware will not work for others. Moreover, developing a decryptor for new ransomware can take a significant amount of time, making this method less effective against new or unknown threats.

The use of expert-created decryptors is one of the most effective ways to recover files encrypted by ransomware, though its applicability is limited to specific cases.

Advantages:

Ease of use: Decryptors can be used by end users without specialised knowledge.

Spot impact: Suitable for fast data recovery if a decrypter for a given ransomware has already been created.

Limitations:

Limited use: Such decryptors are only effective for the known programmes for which they were created.

Developer-dependent: The release of a decrypter depends on how much time has passed since the discovery of the encryptor and on interest in the programme.

4. Machine Learning Methods. The application of machine learning (ML) methods to ransomware decryption relies on the ability of algorithms to identify complex patterns in data (Kharraz A., Robertson W., Balzarotti D., Bilge L., & Kirda E., 2015). ML algorithms can detect patterns and create models that can be used to decrypt new files encrypted by the same ransomware. An example of ML in ransomware decryption is neural networks (Chen J., Bridges R. A., & Ferragut E. M., 2017). Neural networks can be trained on datasets consisting of pairs of encrypted and decrypted files. Once trained, the network can be used to decrypt new encrypted files.

ML methods are promising for ransomware decryption as they can be effective against complex encryption algorithms and are capable of self-learning and adapting to new threats. However, ML methods require large amounts of data for training, which can be a challenge for new or unknown ransomware. Additionally, ML methods may be ineffective against ransomware using advanced encryption techniques, such as key randomization (Rohit K., & Gupta S., 2020).

Despite these challenges, ML methods represent a promising direction for ransomware decryption and could become more effective as ML technologies advance.

Advantages:

Efficiency: artificial intelligence can analyse and identify encryption algorithms faster than is possible manually.

Adaptability: Artificial intelligence algorithms can be adapted for new types of ransomware as they emerge.

Predictive and automatic threat detection: machine learning can identify malware before it is activated and block its actions.

Limitations:

High computing resources: machine learning and artificial intelligence require significant computing power and data to train, which can make them inefficient for small teams.

Training and tuning complexity: Requires careful tuning and training of algorithms, which requires resources and time (Conti M., Dragoni N., & Gottardo S., 2018).

Comparative Analysis of Effectiveness and Limitations.

Table 1. Comparative Analysis of Effectiveness and Limitations

Method	Effectiveness	Time Requirements	Resource Intensity	Limitations
Brute-force	Low	High	High	Ineffective against complex encryption
Vulnerability Analysis	High (if successful)	Significant	Medium	Requires expertise; vulnerabilities may be patched
Expert-Created Decryptors	High for specific cases	Medium	Low	Ineffective against new threats
Machine Learning	Promising	High (for training)	High	Requires large datasets, complex implementation

Note - compiled by the authors

Each ransomware decryption method discussed has its advantages and limitations.

The choice of the optimal decryption method depends on various factors:

– Type of ransomware: Some methods are effective only against specific encryption types.

– Available resources: Time and computational limitations may rule out certain methods.

– Required data recovery speed: In critical situations, speed is a key factor.

Combining methods can increase overall effectiveness. For example, vulnerability analysis can be complemented by machine learning methods to accelerate the process (Sgandurra D., & Muñoz-González L., 2016).

The Role of Artificial Intelligence in Enhancing Decryption Methods.

Artificial Intelligence (AI) and machine learning open up new possibilities in ransomware decryption. AI can be used to automate vulnerability analysis, creating more efficient decryptors. For example, AI algorithms can be trained on datasets containing information about vulnerabilities in various ransomware. These algorithms can then automatically analyze new ransomware and identify potential weaknesses.

AI can also enhance the machine learning methods used for ransomware decryption, optimizing ML algorithms to improve their efficiency. Additionally, AI can develop new machine learning techniques specifically designed for ransomware decryption.

Ultimately, AI could help develop universal decryptors capable of working with a wide range of ransomware. This could be achieved by training AI algorithms on datasets containing information about different ransomware and their encryption methods.

Although AI is not yet widely used for ransomware decryption, it holds great potential for improving existing methods and developing new, more effective solutions. Further research in this area is crucial for combating the growing threat of ransomware.

Conclusion. Ransomware continues to evolve, becoming increasingly sophisticated. Developing effective decryption methods is a critical task in cybersecurity.

This article reviewed the main ransomware decryption methods, analyzing their advantages and limitations. It was shown that there is no universal solution; each method has its specific application and effectiveness. The authors declare that there is no conflict of interest.

Artificial intelligence and machine learning represent promising directions for future research and development. They have the potential to create more effective and adaptive methods for combating ransomware.

Conflict of interest. The author(s) declare that there is no conflict of interest.

References

Shaukat, S., & Ribeiro, B. (2020). RansomWall: A layered defense system against crypto-ransomware attacks using machine learning. Journal of Information Security and Applications, 50, 102583.

Ahmad, A., Webb, J., Desouza, K.C., & Boorman, J. (2019). Establishing a ransomware attack preparedness and response framework. Journal of Organizational Computing and Electronic Commerce, 29 (1), 1-14.

Cybersecurity and Infrastructure Security Agency. (n.d.). Ransomware guidance and resources. Retrieved from https://www.cisa.gov/ransomware.

Europol. (2021). No more ransom celebrates five years of stopping ransomware. Retrieved from https://www.europol.europa.eu/media-press/newsroom/news/no-more-ransom-celebrates-five-years-of-stopping-ransomware.

Mora, S., Bongiovanni, G., Giacinto, G., & Perdisci, R. (2020). Brute-force attack detection: Combining knowledge and data-driven approaches. Computers & Security, 92, 101739.

Al-Rimy, B. A. S., Maarof, M.A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144-166.

Azmoodeh, A., Dehghantanha, A., Choo, K. K. R., & Conti, M. (2018). Detecting crypto-ransomware in IoT networks based on energy consumption footprint. Journal of Ambient Intelligence and Humanized

Computing, 9(4), 1141-1152.

Li, Y., & Guo, L. (2019). Ransomware detection using machine learning algorithms. In Proceedings of the 2019 2nd International Conference on Artificial Intelligence and Big Data (ICAIBD). IEEE, 212-216.

No More Ransom Project. (2021). Free ransomware decryption tools. Retrieved from https://www.nomoreransom.org.

Asghar, M. R., Habib, S., & Javed, M. Y. (2020). Machine learning assisted approach towards ransomware detection. IEEE Access, 8, 114675-114685.

Shaukat, S., & Ribeiro, B. (2018). Ransomware detection using deep learning and autoencoders. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), IEEE, 1-6.

Vinayakumar, R., et al. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525-41550.

Sgandurra, D., & Lupu, E. C. (2016). A survey of machine learning approaches on ransomware detection. Computers & Security, 70, 135-151.

Huang, J., Xu, Z., Chen, Y., & Tang, H. (2020). Enhancing ransomware detection by using convolutional neural network on general-purpose computing on graphics processing unit. Concurrency and Computation: Practice and Experience, 32(16), e5666.

Laszka, A., Farhang, S., & Grossklags, J. (2017). On the economics of ransomware. In International Conference on Decision and Game Theory for Security (pp. 397–417). Springer, Cham.

Cabaj, K., Kotulski, Z., Mazurczyk, W., & Mazurczyk, W. (2018). Detecting ransomware using image similarity metrics. Future Generation Computer Systems, 90, 487–501.

Kolodenker, E., Koch, W., Stringhini, G., & Egele, M. (2017). PayBreak: Defense against cryptographic ransomware. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 599–611.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the Gordian knot: A look under the hood of ransomware attacks. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 3-24). Springer, Cham.

Chen, J., Bridges, R. A., & Ferragut, E. M. (2017). Automated behavior analysis of malware: A case study of WannaCry ransomware. Proceedings of the 2017 IEEE Symposium on Visualization for Cyber Security (VizSec), 1-8.

Rohit, K., & Gupta, S. (2020). AI-driven anti-ransomware approaches for cyber defense. IEEE Transactions on Neural Networks and Learning Systems, 31(7), 2263–2276.

Conti, M., Dragoni, N., & Gottardo, S. (2018). A survey of ransomware and ransomware countermeasures. ACM Computing Surveys (CSUR), 50(6), 1-37.

Sgandurra, D., & Muñoz-González, L. (2016). Anti-ransomware: Measures and countermeasures for high-impact attacks. Proceedings of the 16th IEEE International Symposium on Network Computing and Applications (NCA), 53-58.

Information about authors

Zhaksybek Dias Meirbekuly – doctoral student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, E-mail: zhaksibek.dias@icloud.com, +7 707 809 1053

Akhmetova Zhanar Zhumanovna – PhD, associate professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, E-mail: zaigura@mail.ru*, ORCID: 0000-0002-5483-5260, + 7 778 164 9002

Popov Peter – associate professor, City University London, London, UK, E-mail: p.t.popov@city.ac.uk

Serimbetov Bulat Abutalibovich – candidate of Technical Sciences, Kazakh University of Technology and Business named after K. Kulazhanov, Astana, Kazakhstan, E-mail: sba_rnmc@mail.ru