Safe Bank 1(98) 2025

DOI: 10.26354/bb.5A.1.98.2025

Patryk Król[*]
ORCID: 0000-0003-4079-8849
patkro12@gmail.com

Ransomware as a threat to the security of critical infrastructure, with a focus on the financial system

Abstract

Scientific objective: The aim of this article is to summarise contemporary knowledge of ransomware threats and to examine their impact on critical infrastructure in Poland.

Research problem and methods: The research problem is to analyse the growing threat of ransomware, especially in the context of its impact on public and private institutions. Research methods include a critical analysis of the literature and case studies of actual attacks. Based on the literature review and incident analysis, the paper discusses the stages of a ransomware attack, examples of known incidents in Poland and analyses the level of threat in different economic sectors.

Results: The analysis shows that ransomware has become a serious threat to various sectors, especially critical infrastructure, capable of paralysing institutional operations and causing data leaks.

Conclusions: The author emphasises the urgent need to strengthen security and user education as key defence strategies. He also recommends regular backups and international cooperation in the field of cyber security. The article brings new knowledge on strategies to counter ransomware and emphasises the need for continuous development of security technologies in response to growing digital threats.

Keywords: ransomware, critical infrastructure, critical infrastructure security, financial system, digital threat

JEL Codes: L89

[*] Patryk Król – Poznań University of Economics.

Ransomware jako zagrożenie dla bezpieczeństwa infrastruktury krytycznej, ze szczególnym uwzględnieniem systemu finansowego

Streszczenie

Cel naukowy: Artykuł ma na celu podsumowanie współczesnej wiedzy na temat zagrożeń związanych z ransomware oraz zbadanie ich wpływu na infrastrukturę krytyczną w Polsce.

Problem i metody badawcze: Problemem badawczym jest analiza rosnącego zagrożenia ransomware, zwłaszcza w kontekście jego wpływu na instytucje publiczne i prywatne. Metody badawcze obejmują krytyczną analizę literatury oraz studium przypadków rzeczywistych ataków. Na podstawie przeglądu literatury oraz analizy incydentów, artykuł omawia etapy ataku ransomware, przykłady znanych incydentów w Polsce oraz analizuje poziom zagrożenia w różnych sektorach gospodarki.

Wyniki: Analiza wykazuje, że ransomware stał się poważnym zagrożeniem dla różnych sektorów, szczególnie dla infrastruktury krytycznej, zdolnej do paraliżowania działalności instytucji oraz powodowania wycieków danych.

Wnioski: Autor podkreśla pilną potrzebę wzmocnienia zabezpieczeń oraz edukacji użytkowników jako kluczowych strategii obronnych. Rekomenduje również regularne tworzenie kopii zapasowych oraz współpracę międzynarodową w dziedzinie cyberbezpieczeństwa. Artykuł wnosi nową wiedzę na temat strategii przeciwdziałania ransomware oraz podkreśla potrzebę ciągłego rozwoju technologii zabezpieczeń w odpowiedzi na rosnące zagrożenia cyfrowe.

Słowa kluczowe: ransomware, infrastruktura krytyczna, bezpieczeństwo infrastruktury krytycznej, system finansowy, zagrożenie cyfrowe

Kody JEL: L89

Introduction

One of the more popular types of malware is ransomware[1], which is malware that aims to block the operation, access or prevent the reading of stored data in order to later obtain a ransom from the virus victim (O'Gorman and McDonald 2012). Attacks of this type are on the increase and newer families of ransomware are also being developed. Ransomware is a threat to both individuals and public institutions, where, with the carelessness of the entity responsible for IT network security, the proper operation of the institution can be severely disrupted or prevented. The National Programme for Critical Infrastructure Protection identifies ransomware as one of the potential threats to critical infrastructure security (Government Security Centre 2023). Hackers can also target a country's critical infrastructure with potentially serious and devastating consequences for national security and the operation of critical services. This article aims to summarise the current literature with regard to ransomware threats and provide the reader with key knowledge to understand the fundamental issues relating to this phenomenon. The research methods used in

[1] The name comes from the English words ransom and software.

the article are: a critical analysis of the literature on the subject, an analysis of real, documented attacks on critical infrastructure and an attempt to determine the level of the ransomware threat in Poland.

Pursuant to the Act of 26 April 2007 on crisis management (Journal of Laws 2007, No. 89, item 590), for the purposes of this article, critical infrastructure objects are defined as systems and their constituent functional interconnected objects, including buildings, equipment, installations, services that are key to the security of the state and its citizens and that serve to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs.

1. Stages of a ransomware attack

The European Cyber Security Agency (ENISA) distinguishes four stages of a ransomware attack in its 2022 report:

1. Gaining access – at this stage, the cybercriminal seeks to gain access to the victim's computer system. The malware can be installed on its own, by the victim being misled by phishing methods (King 2024) or by connecting via a remote desktop (Garg, Thakral, Nalwa and Choudhury 2018),[2] exploit kits (O'Kane, Sezer and Carlin 2018), Oracle WebLogic vulnerabilities and vulnerabilities (Snoke and Shimeall 2020), computer worms (Liu, Zhuge and Wu 2018), password cracking (Cobb, Cobb, Kabay and Crothers 2012), code injection[3] (Paul Joseph and Norman 2020) and drive-by installation[4] (Singhal and Levine 2019).
2. Action – ransomware starts by encrypting, blocking access to, deleting or stealing resources stored on the attacked system. These may include files, folders, databases, interface screen, disk memory allocation tables (MFTs), system boot records (MBRs), cloud resources, website content management system (CMS) (ENISA 2022).
3. Blackmail – the cybercriminal makes a demand on the victim to take a certain action, share certain data or, most often, make a payment of a requested sum of money, usually via cryptocurrencies (Kshetri and Voas 2017) or prepaid cards (Simoiu, Bonneau, Gates, Goel 2019), so as to make it difficult to trace the transaction and the perpetrator of the crime.
4. Negotiation – the cybercriminal negotiates the ransom rate with the victim. More often than not, the initial rate is inflated and the victim is left under false time pressure so that they agree to high rates.

[2] Exploit – a vulnerability in software security.

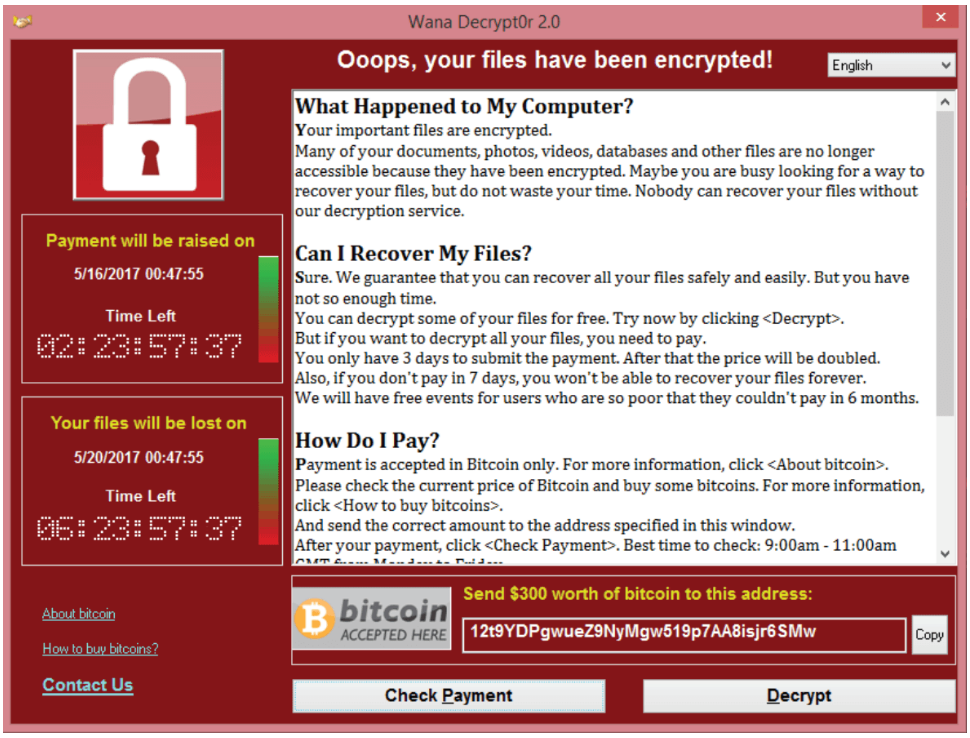
[3] Code injection – a method of attack that exploits a security vulnerability to 'inject' (insert) malicious software code into the victim's software, e.g. SQL injection, XPath injection, LDAP injection (Allodi, Massacci 2014).

[4] Spontaneous installation of malware via an infected website (niebezpiecznik.pl, n.d.).

2. Examples of ransomware attacks

An example of a hacking attack using ransomware against critical infrastructure institutions in Poland is the attack carried out against the Polish Mother's Hospital in Łódź. The attack was carried out by the Lockbit 3.0 group (one of the most active hacker groups). According to Sekurak.pl (2022), backups were also encrypted, and it was possible to leak patients' personal data. A year later, in 2023, the Central Clinical Hospital of the Medical University of Lodz was attacked, also using ransomware, which significantly disrupted the hospital's operations (Sekurak.pl 2023). ENISA, in its report 'Health Threat Landscape' (2023), notes that ransomware accounts for 54% of all security incidents involving the healthcare system. According to this report, 6 cyberattack incidents were reported in Poland between 2021 and the first quarter of 2023, including 1 in 2021, 4 in 2022 and 1 in the first quarter of 2023. A hospital in Pajęczno also fell victim to cybercriminals in 2022, where almost all files were encrypted and cybercriminals demanded a high ransom from the hospital authorities (Sekurak.pl 2022).

Figure 1. WannaCry ransomware interface



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Source: CERT (2017).

In the case of the financial sector, we can note the attack on the Cooperative Bank of Zambrow (Sekurak.pl 2024). The problem of maintaining and setting up IT systems in cooperative banks is highlighted by Kotlinski (2022), who notes that cooperative banks should consider creating common systems uniform for the association or even that post-association solutions should be considered.

Public offices were also victims of ransomware. In the case of the municipality of Nowiny, the databases of the human resources and finance programme were encrypted, and the infection probably occurred at as a result of a municipality employee downloading and installing the malware (Sekurak.pl 2021).

3. Ransomware threat level in Poland

According to CERT Orange (2024), ransomware was the second most frequently detected threat type on the mobile network in 2023, and accounted for 24% of all detections. The most commonly detected threats were adware and HiddenApps, which together accounted for 54% of detected threats. An analysis of the CERT data shows that the highest number of ransomware incidents was reported in business entities, where as many as 81 cases were reported. In second place is public administration with 31 cases, and in third place are private individuals with 30 cases.

The most commonly used ransomware families in Poland are Phobos, which was responsible for 29 incidents, LockBit with 13 incidents and MedusaLocker and Djvu with 7 incidents each. In fifth place is Makop, which was responsible for 6 incidents. The increase in the number of ransomware attacks in Poland can be attributed to several factors. Firstly, increasing digitalisation and reliance on technology are making more and more entities a potential target for cybercriminals. Secondly, the development of encryption technologies and attack tools is making ransomware more sophisticated and more difficult to detect and neutralise.

4. Main methods of ransomware prevention

Beaman, Barkworth, Akande, Hanak and Khan (2021) distinguish two main categories of ransomware countermeasures:

1. Prevention and mitigation, which involves stopping or reversing the effects of ransomware. These methods include:
    a. Backups – enabling the system to be restored to its state prior to the computer attack; cyclical backups are required for this method to work,
    b. Obtaining the decryption key – with some types of software, the decryption key can be obtained from its files. In a study by Bajpai and Enbody (2020), who conducted a side-channel attack on malware, this method achieved 100% success against ransomware such as NotPetya, WannaCry, LockCrypt, CryptoRoger. There are also reported cases of keys being obtained by breaking up a cybercrime group.
    c. User awareness – educate users on the dangers of ransomware and best security practices, such as avoiding opening suspicious attachments and clicking on unknown links, which can prevent infections.

   d. Network segmentation – segmenting the network to limit the spread of ransomware in the event of infection. This makes it harder for malware to access critical resources, which can minimise damage.
   e. Access control – implementing strict access control policies such as multi-level authorisation and limiting user rights to the minimum necessary to perform their duties, making it difficult for ransomware to gain administrative rights and encrypt the entire system.
2. Ransomware detection:
   a. Machine learning
   b. Honeypot
   c. Network traffic analysis
   d. File analysis
   e. Analysis of reports of ransomware
   f. The machine is finished
   g. Analysis of the IT system (e.g. Windows registry keys and system logs)

5. Potential actions

If the system is infected, CERT (2021) recommends the following actions:

1. Isolation of the infected machine, preventing the virus from spreading to uninfected systems.
2. Identification and elimination of infections.
3. Identification of the ransomware family.
4. Restore system operation.
5. Report the incident to the NASK CSIRT team, to which a minimum of 2 encrypted files and a note with the ransom demand from the offender should be attached. It is also recommended to send a sample of the malware, logs from the infected machine and security systems, as well as the originals of the infected files, if available.

CERT also provides a free tool from recovering the ransomware Vortex encryption key.

For ad hoc actions (especially if the institution decides to negotiate with offenders), the NCC study (2021) recommends the following:

1. If a staff member notes an infection, do not continue the interaction so as not to activate the timer.
2. Decisions should not be made under time pressure, despite the pressure exerted by offenders. Requests to give victims more time are usually effective.
3. Cybercriminals often agree to ransom amounts less than initially requested (e.g. USD 350,000 instead of USD 1 million). In the NCC study, messages from the victim company about their low income and inability to pay the requested amount, along with a proposal for an alternative, smaller ransom amount, were effective.

4. Do not inform cyber criminals that you have ransomware insurance.
5. An external communication channel should be established to prevent interference and interference by third parties.
6. Cybercriminals often share information about system vulnerabilities within a company if they are asked for it by a victim who has agreed to pay a ransom.

It should be noted here that deciding to pay the ransom, in whole or in part, does not guarantee that the data will be unlocked and the system restored to working order. It should therefore be considered as a last resort, in cases where it is necessary to restore the proper functioning of the institution and the data is impossible to recover or restore by any other means. Guidance on negotiating with cybercriminals is included in this article because, according to the ENISA report (2023), more than 60% of victims of ransomware attacks may have chosen to pay the ransom. The information is therefore important from the perspective of reducing the severity of the attack. CERT (2017) does not recommend paying the ransom, but recommends restoring the system using a backup or moving the infected data to a separate drive and reinstalling the infected operating system to enable decryption of the data without paying the ransom in the future.

Summary

Ransomware is a growing threat to digital security that involves blocking access to data and demanding a ransom to unlock it. The article analyses cases of ransomware attacks on critical infrastructure in Poland, examining both the technical aspects of these attacks and their consequences for the affected entities. Using a case study analysis, the author highlights the increasing complexity and effectiveness of these attacks and their significant impact on the operations of public and private institutions.

Research shows that the key stages of an attack include gaining access to a system, spreading malware, encrypting data and demanding a ransom. The examples of attacks discussed demonstrate the variety of methods used by cybercriminals, from phishing to advanced exploits.

Based on the article, we can therefore identify five main recommendations:

1. Strengthening security: institutions should invest in advanced security systems, regularly update software and apply multi-layered defence strategies against ransomware attacks.
2. Employee training: educating employees on how to recognise phishing attempts and other social engineering methods is key. Regular training can significantly reduce the risk of a successful attack.
3. Regular backups: making regular backups of data and storing it securely offline can significantly reduce the impact of a ransomware attack. Institutions should develop and test data restoration plans.

4. International cooperation: increased international cooperation in sharing threat information and best practices can help to respond more quickly to new types of ransomware attacks.
5. Research and development: continued research into new methods of detecting and neutralising ransomware, as well as the development of security technologies, is essential to maintain an edge over cybercriminals.

In conclusion, the article demonstrates the urgent need for comprehensive measures to increase resilience against ransomware attacks. Adopting proactive strategies and continuously improving defensive measures can significantly reduce the risk and impact of these attacks, protecting both data and the business continuity of key institutions.

Bibliography

Allodi L., Massacci F. (2014), *Comparing vulnerability severity and exploits using case-control studies*. ACM Transactions on Information and System Security (TISSEC), 17(1), 1–20.

Beaman C., Barkworth A., Akande T.D., Hakak S., Khan M.K. (2021), *Ransomware: Recent advances, analysis, challenges and future research directions*. Computers & security, 111, 102490.

CERT (2017), WannaCry Ransomware, Downloaded from: https://cert.pl/posts/2017/05/wannacry-ransomware/ (accessed 12.07.2024).

CERT (2021), Ransomware guide.

CERT (2024), Annual report on the activities of CERT POLSKA 2023.

CERT Orange Polska (2024), CERT Orange report for 2023.

Cobb C., Cobb S., Kabay M.E., Crothers T. (2012), *Penetrating computer systems and networks*. Computer Security Handbook, 15-1.

ENISA (2020), Ransomware ENISA Threat Landscape.

ENISA (2023), ENISA Threat Lanscape: Health Sector

Garg D., Thakral A., Nalwa T., Choudhury T. (2018), *A past examination and future expectation: Ransomware*. In 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE) (pp. 243–247), IEEE.

Król P. (2024), *Phishing as a threat to digital banking security*. Bezpieczny Bank 1(94), 25–42. https://doi.org/10.26354/bb.2.1.94.2024

Kshetri N., Voas J. (2017), *Do crypto-currencies fuel ransomware?*, IT professional, 19(5), 11–15.

Liu Y., Zhuge J., Wu Y. (2018), *Threat and defense of new ransomware worm in industrial control system*. Journal of Computer Applications, 38(6), 1608.

NCC (2021), "We wait, because we know you." Inside the ransomware negotiation economics, https://research.nccgroup.com/2021/11/12/we-wait-because-we-know-you-inside-the-ransomware-negotiation-economics/ (accessed 6.07.2024).

Niebezpiecznik.pl (n.d.), *Do you have an Android? Beware of drive-by-download attacks*, https://niebezpiecznik.pl/symantec/masz-androida-uwazaj-na-ataki-drive-by-download/ (accessed 6.07.2024).

O'Gorman G., McDonald G. (2012), *Ransomware: A growing menace*. Arizona, AZ, USA: Symantec Corporation.

O'Kane P., Sezer S., Carlin D. (2018), *Evolution of ransomware*. Iet Networks, 7(5), 321–327.

Paul Joseph D., Norman J. (2020), *A review and analysis of ransomware using memory forensics and its tools*, [in:] *Smart Intelligent Computing and Applications*. Proceedings of the Third International Conference on Smart Computing and Informatics, Volume 1 (pp. 505–514), Springer Singapore.

Government Security Centre. (2023), National Programme for the Protection of Critical Infrastructure: Annex 1. Standards to ensure the smooth functioning of critical infrastructure – good practices and recommendations, https://www.gov.pl/attachment/02553b90-184a-42c5-8445-5f9b1f0b74ee

Sekurak.co.uk (2021), Ransomware and leakage in the municipality of Nowiny. Retrieved from: https://sekurak.pl/ransomware-i-wyciek-w-gminie-nowiny/ (accessed 6.07.2024).

Sekurak.co.uk (2022a), *Polish Mother's Hospital in Lodz infected with ransomware. They also report a 'possible leak'*, https://sekurak.pl/szpital-matki-polki-w-lodzi-zainfekowany-ransomware-informuja-rowniez-o-mozliwym-wycieku/ (accessed 6.07.2024).

Sekurak.co.uk (2022b), *Ransomware in a hospital in Pajęczno: There was an 'unexpected IT system failure'*, https://sekurak.pl/ransomware-w-szpitalu-w-pajecznie-nastapila-niespodziewana-awaria-systemu-informatycznego/ (accessed 6.07.2024).

Sekurak.co.uk (2023), *Cyber attack on the Central Clinical Hospital of the Medical University of Lodz*, https://sekurak.pl/cyberatak-na-centralny-szpital-kliniczny-uniwersytetu-medycznego-w-lodzi/ (accessed 6.07.2024).

Simoiu, C., Bonneau, J., Gates, C. and Goel, S. (2019), "*I was told to buy a software or lose my computer. I ignored it": A study of ransomware*, [in:] *Fifteenth symposium on usable privacy and security (SOUPS 2019)* (pp. 155–174).

Singhal M., Levine D. (2019, October), *Analysis and categorization of drive-by download malware*, [in:] *2019 4th International Conference on Computing, Communications and Security (ICCCS)* (pp. 1–4), IEEE.

Snoke T.D., Shimeall T.J. (2020), *An updated framework of defenses against ransomware*. Technical report, Carnegie-Mellon Univ Pittsburgh, PA.