# Brain Cipher Ransomware Attack Reveals Critical Gaps in National Cybersecurity

Yoyok Darmanto[1*], Rahmat Rian Hidayat[2], Ardian Setio Utomo[2]

[1]Directorate of Cryptographic Operations, National Cyber and Crypto Agency, Depok, Indonesia

[2]Information Communication Management Study Program, Sekolah Tinggi Multi Media, Yogyakarta, Indonesia

*Coressponding Author Email: yoyok.darmanto@bssn.go.id

**Abstract.** General Background: Cyberattacks targeting critical digital infrastructure pose significant threats to national security, public services, and digital sovereignty. Specific Background: The June 2024 Brain Cipher ransomware attack on Indonesia's National Data Center (PDNS 2) in Surabaya, executed using a LockBit 3.0 variant, disrupted over 200 public services and exposed systemic vulnerabilities. Knowledge Gap: Despite the scale of the incident, there is limited integrated analysis combining technical reconstruction, impact assessment, and strategic cybersecurity lessons from this attack. Aims: This study aims to provide a comprehensive technical analysis, evaluate the impact, and derive national cybersecurity lessons from the Brain Cipher ransomware incident. Results: Using a qualitative case study with a Digital Forensics Review (DFR) approach, the analysis confirms that 282 government institutions were affected, disrupting essential services such as immigration and taxation. The attack exploited remote access points for data encryption, while emergency recovery relied on AWS migration and Batam-based backups, revealing external dependencies. Novelty: This study offers an integrated examination of a large-scale ransomware incident by combining forensic reconstruction, impact evaluation, and policy-oriented cybersecurity insights. Implications: The findings emphasize the need for geographically redundant infrastructure, automated failover testing, behavior-based detection systems (EDR/XDR), and the institutionalization of security culture to strengthen national cyber resilience and safeguard digital sovereignty.

**Keywords**:Ransomware attack; Digital forensics analysis; National cybersecurity; Critical infrastructure security; Brain Cipher ransomware

## 1 Introduction

Ransomware has evolved into the dominant threat to digital infrastructure in the past five years, especially in government sectors that manage large-scale information systems[1], [2]. Attacks carried out by groups such as LockBit 3.0 demonstrate significant improvements in technical capabilities, including *modular payload* capabilities, *anti-forensics* mechanisms, and *triple extortion tactics* that force victims


R. Lomotey et al. (eds.), *Proceedings of the 1st International Conference on Communication and Digital Multimedia 2025 (ICCDM 2025)*, Advances in Social Science, Education and Humanities Research 1020,
https://doi.org/10.2991/978-2-38476-589-8_15

through the threat of data leaks[3]. This global trend puts public organizations at greater risk, given that governments' reliance on digital services continues to increase every year [4], [5]. In the Indonesian context, the Brain Cipher ransomware attack on the Temporary National Data Center (PDNS) 2 Surabaya in June 2024 is a vivid illustration of such a threat, and shows the immediate consequences when strategic infrastructure is not protected by an adequate cyber defense system [6], [7].

Previous research has examined the technical behavior of LockBit 3.0, including infiltration methods, encryption, and camouflage techniques to avoid antivirus detection[8], [9], [10]. However, there is a literature gap regarding *the intermittent encryption* mechanism that is now implemented by modern ransomware variants [11]. This technique only encrypts a small part of the file while the rest is left unchanged, so that the encryption process can run much faster and not trigger a significant increase in entropy in the file [12]. Some studies report that this technique is increasingly difficult to detect by traditional behavior-based security systems, as byte change patterns do not fully reflect ransomware attacks [13] . This condition shows the need for a more in-depth analysis of the use of partial encryption in real-world events such as the PDNS 2 attack [6], [14], [15].

Preliminary findings from the PDNS 2 incident show that Brain Cipher implemented a partial encryption pattern by consistently modifying the initial block of the file up to an offset of 0x80000 (512 KB) and adding a change of 288 bytes to the end area of the file [16]. This technique is very similar to the pattern described in the literature regarding new-generation ransomware such as BlackCat and Babuk, which use partial encryption to increase the speed of attacks in large-scale data center environments [17]. However, there have been no academic publications that have specifically analyzed the implementation of the technique in the real context of Indonesia, especially on attacks involving national data centers. Thus, there is still an important need to map the technical patterns of Brain Cipher empirically to strengthen the existing knowledge base [16].

The urgency of the research is heightened because Brain Cipher's operational tactics appear to be highly systematic and exploit a variety of critical vulnerabilities, including the disabling of Windows Defender, the removal of Volume Shadow Copy Service (VSS), and the exploit of CVE-2023-28252 that allowed the escalation of access rights on Windows systems [18], [19], [20]. This shows that the perpetrators not only rely on encryption capabilities, but also integrate elements of *defense evasion* and *privilege escalation* at the operating system level. The impact of the attack on PDNS 2 extended to 282 government agencies and caused disruption to essential services such as immigration, taxation, and government logistics [15], [6] . This situation serves as a strategic warning that partial encryption techniques are not only a technical innovation, but also increasingly play a role in the operational effectiveness of ransomware attacks [16], [12].

Based on this background, this study aims to provide a comprehensive analysis of the Brain Cipher encryption pattern through a hexadecimal forensic approach. This approach allows for the identification of broken and unbroken binary structures, so that partial encryption patterns can be revealed more measurably [12], [16]. In addition, this study also evaluated the potential for *partial recovery* in several file types to assess the extent to which intact data can be restored [19]. The contribution of this research not only expands the academic literature on partial encryption techniques, but also provides

a methodological framework for forensic analysis of ransomware incidents at the national and international levels [21], [18].

This study uses a descriptive qualitative approach with a case study method to analyze encryption patterns, technical impacts, and potential data recovery from the Brain Cipher ransomware attack that occurred at PDNS 2 Surabaya in 2024. The case study approach was chosen because the research focuses on a single complex real-life incident, involving digital artifacts, forensic evidence, as well as technical patterns of encryption that can only be understood in depth through the exploration of specific contexts. This approach allows researchers to combine various data sources, such as technical reports, malware samples, infected files, and hexadecimal analysis results to obtain a comprehensive picture of the attack process, this is as depicted in figure 1.


**Fig. 1.** Research Stages

**Research Setting and Data Sources.** The research was conducted by analyzing technical data from the PDNS 2 Surabaya incident which occurred on June 20-24, 2024. Primary data includes:

1. A sample of the Brain Cipher ransomware in the form of *an executable* that originated from the site of the infection.
2. Encrypted files of various formats (PDF, DOCX, TXT, MP3, SQL) with new extensions added by ransomware.
3. Encryption logs and malware execution results in a sandbox environment.
4. Technical documents such as MITRE ATT&CK mapping, compromise indicators (IOCs), as well as security organization reports (ASIS, SentinelOne, Peris.ai).

Secondary data comes from technical publications and security vendor reports documenting the characteristics of Brain Cipher and LockBit 3.0. Digital artifact-based purposive sampling techniques are used for the selection of analyzed malware files and samples. The selection of artifacts is carried out based on the following criteria:

1. Encrypted files that have the original vs infected file equivalent.
2. Files of different sizes to test partial encryption patterns (e.g. blank PDF, large PDF, MP3 audio, large SQL).
3. Sample files showing technical anomalies (offset changes, fixed data, broken structure).

This sampling approach is in accordance with digital forensic research standards, where research objects are selected based on their technical relevance to the objectives of the investigation. Data collection is carried out through three techniques:

1. File-Based Static Analysis, use the HxD Hex Editor to compare the binary structure between the original and encrypted files. Activities include looking at the beginning–end offset, identify byte changes, detect encryption patterns, determine the area that has not changed. The report indicates that the author started the analysis from the end of the file and found an unencrypted offset on the 0x329760 region, which is identical to the original file ().
2. Dynamic Malware Execution (Sandbox Test), the ransomware sample is run in an isolated environment to monitoring the encryption process, observing changes in file extensions, view the behavior of the dropper and the Brain Cipher payload.
3. Document & Log Analysis, analyzed system logs, Windows Defender shutdown reports, VSS removals, and CVE-2023-28252 calls. Additional documents of MITRE ATT&CK are used to map attack techniques.

**Data Validation.**Validation was carried out using triangulation methods and source triangulation, namely:

1. Triangulation method, comparison between static analysis (offset) vs dynamic analysis (encryption pattern).
2. Verify the encryption pattern by attempting manual recovery.
3. Source triangulation, comparing the results of the analysis with the reports of SentinelOne, Peris.ai, and ASIS International

This triangulation approach is commonly used in digital forensic research to improve the reliability of results.

**Data Analysis Techniques.**Data analysis was carried out using thematic technical analysis methods and hexadecimal comparative analysis, including:

1. Identification of Technical ThemesThemes such as "partial encryption", "offset boundary", "encryption header damage", and "recovery potential" emerged from the observations.
2. Comparative Hexadecimal Analysis by calculate the offset difference (e.g. 0x120 = 288 bytes), converts the 0x80000 offset to 512 KB, detects consistent encryption limits.
3. File Structure Reconstruction by retrieves whole blocks of data (e.g., 0x80000–0x329760), reorder files to obtain partial recovery.
4. Cross-Format Analysis, assess encryption patterns on PDF, DOCX, TXT, MP3, SQL

This analysis method combines a qualitative thematic approach with technical procedures commonly used in digital forensics research.

## 2 Discussion

On June 20, 2024, Indonesia was shaken by a massive cyberattack targeting one of its most critical digital infrastructures the Temporary National Data Center (PDNS 2) in Surabaya. The attack was carried out by the Brain Cipher group, a new variant of the LockBit 3.0 ransomware family, which encrypted thousands of government systems and crippled numerous public services. According to ASIS International's report, Brain Cipher employed sophisticated tactics and techniques to breach the national server

defenses [22]. The incident became a major wake-up call for Indonesia's cybersecurity resilience.

Phase 1, Infiltration & Exploitation Investigations revealed that the attack began around June 17, 2024, when security features such as Windows Defender were disabled across several PDNS 2 servers. By June 20, the malware had become fully active, encrypting data across storage systems and virtual servers [23]. The exploitation leveraged vulnerabilities in Windows systems notably CVE-2023-28252 allowing attackers to execute arbitrary code with administrative privileges [24].

Phase 2, Propagation & Encryption Copy Once full access was achieved, Brain Cipher disabled security services and the Volume Shadow Service (VSS) to prevent data recovery. The malware then encrypted critical files including virtual disks, Veeam backups, and Hyper-V snapshots — using its unique extension format.

Phase 3, Ransom & Key Disclosure The Brain Cipher group demanded a ransom of USD 8 million (approx. IDR 131 billion) in exchange for the decryption key [25]. The Indonesian government refused to pay, focusing instead on internal recovery efforts [26]. "The team in charge of investigating the cyberattack found that PDNS 2 was attacked by a new ransomware called Brain Cipher." Budi Arie Setiadi, Minister of Communication and Information Technology (June 24, 2024) [27].

Brain Cipher is a modified build of LockBit 3.0, created using the leaked LockBit builder tool. The ransomware is capable of [24]:

1. Deleting restore points and automatic backups
2. Using advanced obfuscation to conceal activity
3. Communicating via the TOR network and accepting payments in Monero (XMR)
4. Targeting Windows Server and virtualized infrastructure environments

The Technology & Tactics (MITRE ATT&CK Mapping) as shown in Table 1.

**Table 1.** Technology & Tactics (MITRE ATT&CK Mapping)

| No. | Phase | Technical | ID | Information |
|---|---|---|---|---|
| 1 | Initial Access | Exploit Public-Facing Application | T1190 | Exploit public application vulnerabilities |
| 2 | Execution | Command Shell / Script Dropper | T1059.003 | Run encrypted payloads |
| 3 | Privilege Escalation | Abuse of CVE-2023-28252 (CLFS Driver) | T1548.002 | Getting system admin rights |
| 4 | Defense Evasion | Disable Security Tools & VSS | T1562 | Prevent detection and recovery |
| 5 | Impact | Data Encryption for Impact | T1486 | Encrypt data with a unique per-machine key |

Forensic analysis of the Brain Cipher incident in PDNS 2 identified a number of indicators of compromise (IOCs) that are the main markers of the presence and activity of ransomware in the system environment.The analyzed ransomware sample had a SHA-256hash ofeb82946fa0de261e92f8f60aa878c9fef9ebb34fdababa66995403b110118b12, which serves as a cryptographic identity for verifying the presence of malware on various hosts or digital repositories. In addition, command-and-control (C2) communications were detected to be directed to the IP address 199.232.214.172, which is located in the United States, and acts as a control server for payload retrieval and encryption telemetry delivery. Another artifact found is the existence of a file dropper named Lockbit3_build.exe, which has undergone a repacking process to disguise the original source and avoid signature-based detection. These three indicators are critical components in the process of early detection, isolation, and incident response to the Brain Cipher ransomware variant. This analysis will help understand the nature of the encrypted data, the potential for recovery, and the steps that have been taken to try recovery.[28]

**Hexadecimal Comparison and Offset Analysis.** After the Brain Cipher malware was active and began encrypting various files and data on the victim's computer, the author found something quite interesting. There is a strangeness that begs the question: *how can a single data center be encrypted so quickly?* Is it true that all data is really encrypted, or is it that the perpetrator uses another approach?

From this curiosity, the author then seeks to delve deeper to understand the difference between data that has been encrypted and that has not. For this reason, the author uses the HxD tool (Hexa Editor) to compare the representation of hexadecimal to decimal, so that it can be analyzed in more detail about the encryption pattern that occurs. In this analysis, the author begins the examination of the hexadecimal value at the end of the file. From the observations, it was found that the Brain Cipher ransomware did not fully encrypt the entire contents of the file. This is evidenced by the 0x329760 and above offsets, where the content of the data in the encrypted file is still exactly the same as the content of the data in the original file that has not been encrypted. As such, it can be concluded that this ransomware only encrypts a partial block of data most likely to speed up the attack process without the need to encrypt the entire file. The result is a value of 0x120 (hexadecimal), which when converted yields 0x120 (hexa) = 288 (desimal), 288 bytes = 0.28125 kilobytes (KB) or about 0.28 KB. In other words, the ransomware only encrypts about 288 bytes of a specific part of the file.

This 288 bytes is very small when compared to the file size of .mp3 which generally reaches a few megabytes. This fact reinforces the previous finding that the Brain Cipher ransomware does not perform end-to-end encryption, but rather only encrypts a small portion of data in a specific area usually at the beginning or end block of a file, which contains important structures (such as headers or metadata).

By simply changing such a small block, the perpetrator can still make the file unplayable or unreadable because the vital parts that determine the file format have been corrupted. This method is known as the partial encryption technique, and is a common strategy in modern ransomware (e.g. LockBit, BlackCat, or Phobos) to:

1. Speed up the bulk encryption process on thousands of files on servers or data centers.
2. Saves CPU and I/O resources, making encryption activity difficult for monitoring systems to detect.
3. Inflicts significant damage with minimal time just change a small portion of the file to make the entire data inaccessible.

In other words, the data portion on the 0x80000 downward offset does not undergo the encryption process and still retains its original structure. These findings further strengthen the indication that ransomware does not encrypt the entire contents of the file, but only a certain part of the block at the beginning of the file.

This approach is generally used to speed up the bulk encryption process without the need to change the entire data, but still cause the file to become corrupted and unable to open because important headers or metadata have been affected. The offset value 0x80000 in a hexadecimal system when converted to decimal yields 524,288 bytes, or the equivalent of 512 KB (kilobytes). This figure is no coincidence — many modern ransomware variants use certain encryption limits (e.g. 256 KB, 512 KB, or 1 MB) as an efficiency strategy. In this context, the Brain Cipher ransomware appears to only encrypt the initial part of the file up to the first ±512 KB in size. This approach has several important technical implications:

1. By, encrypting only the initial block (e.g. 512 KB), ransomware can process thousands of large files much faster than encrypting the entire file. For data centers such as PDNS Surabaya that have large data volumes, this method allows attacks to take place in minutes.
2. Maximum Functional Breakdown, many file formats (such as MP3, DOCX, ZIP, and PDF) store the header structure and metadata index at the beginning of the file. Changing the first block to an offset 0x80000 is enough to break the internal structure of the file, so the file cannot be recognized or played by the system even though most of the data is intact.
3. Partial Encryption Efficiency, this type of ransomware typically applies a stream cipher or block cipher algorithm (e.g. AES-256 in CBC or CTR mode) to some of the initial data, and then leaves the rest of the block unmodified.
   That way, perpetrators can save time and resources while still ensuring that victims lose access to data.
4. Forensic Signature, a stop encryption pattern on fixed offsets such as 0x80000 can be a unique indicator (Indicator of Compromise / IOC). When forensically analyzed, it helps identify specific ransomware variants or even trace the reverse engineering patterns used by the perpetrators.

Based on the results of the analysis using HxD Hex Editor, it is known that the ransomware does not encrypt the entire file, but only a portion of the data block at a certain offset. From the observation results on the mv56ALfcQnujI.mp3 file which is compared with the original Peterpan The Deepest (Official Music Video) file.mp3, it can be seen that:

1. The encryption process is only done before the 0x80000 offset.
2. Offsets below 0x80000 (i.e. from 0x00000 to 0x7FFFF) are unchanged, so they remain in their original state (unencrypted).

Furthermore, recovery of files that have been infected with ransomware is carried out by restoring unencrypted data blocks in the offset range of 0x80000 to 0x329760. This recovery aims to restore some of the file structure that is still recognizable and readable by the system, although other parts remain corrupted by the ransomware encryption process. From the image, it can be seen that the process of selecting data blocks using *the Select Block* feature on HxD, with the following parameters:

1. Start-offset: 0x80000
2. End-offset: 0x329760
3. Length: 0x249761

Through this process, it can be concluded that ransomware applies partial encryption, that is, not all of the contents of the file are encrypted, but only part of the initial or middle block of the file to save processing time but still make the file unusable. This kind of analysis is useful for identifying encryption patterns, allowing partial recovery of data that has not been affected by full encryption.

Recovery is carried out in a way that Return a block of data on an offset that has not been subjected to the encryption process, as identified in the previous analysis (offsets below 0x80000 are still in the original state).

The results in the image show a representation of binary data in hexadecimal format and decoded text. It shows a byte pattern that is still consistent and not random, indicating that the data in this area has not been encrypted by ransomware. Thus, this section can still be considered valid data that has the potential to be restored through the file reconstruction process.

Technically, the success of displaying shows that:

1. Ransomware does not fully encrypt the entire file, but only a certain part (partial).
2. The initial offset of the file up to before the 0x80000 is still accessible and readable without interruption, which means that the structure of the MP3 file in the header and part of the audio frame is intact.
3. The data displayed in the hexadecimal editor shows byte patterns typical of MP3 formats (e.g. FF FB or FF F3 prefixes in audio frames), which can be used as a reference for advanced reconstruction processes.

This analysis is important because from a digital forensic point of view, the identification of areas of data that are still intact allows:

1. Attempts to partially recover encrypted files,
2. Understanding ransomware encryption patterns, and
3. Development of more effective mitigation or decryption strategies in the future.

According to guidelines from the *National Institute of Standards and Technology (NIST SP 800-86),* this stage of analysis is included in the process of "data carving and recovery", which is an effort to extract data that is still valid from media or files that have been damaged by a cyberattack.

In the directory you can see some files with the extension .flzQGnjIJ, which is a new extension generated by the ransomware after the encryption process is complete. The file is an encrypted version of the original data that was previously on the victim's system. From the observations, the audio file with the original name "Peterpan - The

Deepest (Official Music Video).mp3" was partially recovered. This is characterized by the presence of two versions of the file:

1. The original files that have been infected (Peterpan - The Deepest (Official Music Video).mp3.flzQGnjIJ), and
2. Reconstruction or restoration files (Peterpan - The Deepest (Official Music Video) partial recovery.mp3).

Perform advanced experiments on multiple file types that have been encrypted by applying the same file recovery method as previously described this is as depicted in table 2, 3, 4, 5, 6.

**Table 2.** Recovey File .PDF Extension

| Type | File Size Beginning (KB) | Recovery Action | Result | Information |
|---|---|---|---|---|
| Empty | 13 | Replace extensions | Not can Opened or Not exist yard | File beginning .Pdf 1 Plain Pages |
| Usual | 1380 | Replace extensions | Recover thing 105-end | - |
| | | Delete the initial 32 KB of encrypted files then replace the extension | Recover page 105-end | - |
| | | Delete the initial (32 KB) and the end (+- 280B) of encrypted files then replace the extension | Recover page 105-end | - |
| Signed | 21317 | Replace extensions | Not can Opened or Not can Displaying pages | - |

**Table 3.** Recovey File Extension .docx

| Type | File Size Beginning (KB) | Recovery Action | Result | Information |
|---|---|---|---|---|
| Empty | 13 | Replace extensions | Cannot be opened | File beginning .docx 1 Plain Pages |
| Usual | 1380 | Deletes the initial (32 KB) and end (+-280B) of encrypted files later Replace extensions | Cannot be opened | - |

**Table 4.** Recovey File yang Extension .Txt

| Type | File size Beginning (KB) | Action Recovery | Result | Information |
|---|---|---|---|---|
| Empty | 0 | - | Unencrypted | Not processed by ransom |
| Mini | 1 | Open using Text editor | Increased file size | - |
| Usual | 31 27 | Open using the text editor | The initial part of the encrypted file and the addition at the end File | - |

**Table 5.** Recovey File Extension .mp3

| Type | File size Beginning (KB) | Action Recovery | Result | Information |
|---|---|---|---|---|
| Usual | 1818 | Delete the initial section (32 KB) and section end (+-280B) File encrypted then Replace extensions | Can be recovered with the initial part cut off | - |

**Table 6.** Recovey File Extension .sal

| Type | File size Beginning (KB) | Action Recovery | Result | Information |
|---|---|---|---|---|
| Usual | 1207 | Replace the initial 32KB file with a sql template file format, Replace the extension | *Top sourcecode* and about 2000 **user** lines disappear. | - |

**Impact and Government Response.**The Brain Cipher attack on PDNS 2 had a very wide impact on the operations of Indonesian government services. A total of 282 government agencies were directly affected by the system disruption, causing the suspension of various public services that required access to the national database. The most critical impacts occurred in the immigration, taxation, and staffing services sectors, where administrative processes could not run because the backend system was inaccessible. This condition has led to real disruptions in the field, including long queues at airports due to a crippled immigration system, slowing down the process of checking travel documents. This situation illustrates the level of dependence of public services on central digital infrastructure, while also confirming the vulnerability of systems when not supported by adequate security architectures and recovery strategies [29].

In response to the incident, the Ministry of Communication and Information Technology (Kominfo) together with the State Cyber and Cryptography Agency (BSSN) formed a special forensic team to investigate the pattern of attacks and ensure that the perpetrators did not come from state actors, but from organized cybercriminal groups. The government then took emergency recovery steps through migrating temporary services to AWS Cloud and utilizing data backup providers in Batam to ensure the sustainability of public services while the repair process is carried out. As part of moral responsibility for the attack, the Director General of Informatics Applications of Kominfo submitted his resignation, indicating the government's seriousness in evaluating national cybersecurity governance and increasing public trust in recovery efforts [30].

## 3 Conclusion

The Brain Cipher attack at PDNS 2 Surabaya was not just a technical incident it was a national warning that *digital sovereignty* is just as important as territorial sovereignty. "Data security is not only the responsibility of the central government, but the entire Indonesian digital ecosystem." Going forward, the challenge is not just to restore systems, but to build sustainable national cyber resilience where security is the DNA, not the reaction. From the results of the calculation and hexadecimal analysis, it can be concluded that technically, these findings reinforce previous analysis that:

1. The changed offset is only 288 bytes (≈0.28 KB).

2. This means that this ransomware does not encrypt the entire contents of the file, but only certain parts that are strategic.
3. This approach indicates the existence of an attack efficiency mechanism, which aims to accelerate mass encryption in the PDNS Surabaya data center environment.
4. Brain Cipher encrypts the initial block up to about the first 512 KB of each file.
5. The offset 0x80000 be the logical boundary at which the encryption process stops.
6. The part after that offset remains unencrypted, but the file remains unusable because the critical structure at the beginning of the file has been tampered with.
7. Based on the results of follow-up observations of the infected file set, a pattern was found that files with a size below 512 KB could not be recovered at all. This happens because ransomware fully encrypts small files.
8. By understanding these patterns, forensic analysts can devise more accurate methods of early detection and mapping of the impact of encryption, including the potential for partial recovery of blocks of data that are not affected by encryption.
9. The Brain Cipher ransomware does not fully encrypt the entire file. This partial encryption is performed only at the initial part or a specific block, to speed up execution time and save resources.
10. Unencrypted data can still be manually reconstructed using a hexadecimal editor such as *HxD*, by extracting uncorrupted blocks and rearranging them into the original file format.
11. This process results in files with partial integrity, where some of the content can still be played or accessed, even if the internal structure is not completely intact.

**Important Lessons and Technical Recommendations.**The Brain Cipher attack incident on PDNS 2 provides a number of important lessons for strengthening national cybersecurity, especially related to the country's dependence on one physical data center. This case shows that strategic infrastructure should not be centralized in one location, as a single point of failure can paralyze hundreds of public services simultaneously. In addition, this incident exposed a weakness in data backup management, where backup systems were supposed to be tested automatically through *routine* failover procedures to ensure they could function when a critical outage occurred. From a technical defense standpoint, the findings also underscore that behavior-based detections such as EDR/XDR are much more effective than conventional antiviruses, which often rely solely on signatures and fail to detect new malware variants with partial encryption techniques. Beyond the technical aspects, the PDNS 2 incident reflects the need for significant improvements in the cybersecurity culture in government agencies, including consistent training, policies, and security discipline to minimize the risk of procedural errors and operational negligence. This lesson underscores that strengthening the security architecture, technology, and culture is the main foundation to prevent the recurrence of similar incidents on national digital infrastructure in the future.

**Recommendations**

1. Network segmentation: separate public systems and critical data in different *network zones*.
2. 3–2–1 backup strategy: three copies, two media, one *offsite/hot site*.
3. EDR/XDR implementations that monitor the abnormal behavior of the system.

4. Routine incident simulations and *tabletop exercises* for technical officials.
5. Periodic independent audits with the publication of results at a minimum of aggregate level.
6. User awareness training to reduce the risk of *phishing* and *social engineering*.
7. The DR/BCP (Disaster Recovery & Business Continuity) plan is integrated for all national digital services.

**Acknowledgements.** We would like to thank the colleagues from the Badan Sandi dan Siber Negara and Sekolah Tinggi Multi Media Yogyakarta who provided valuable insights and expertise for this research, even though they may not agree with all the interpretations in this paper. The author is grateful for the support provided by the Manajemen Informasi Komunikasi, Sekolah Tinggi Multi Media Yogyakarta (the author's affiliation) and Badan Siber dan Sandi Negara throughout this research.

## References

[1] B. Olosunde, "Ransomware Threats to Critical Infrastructure in the USA," *IJISET-International J. Innov. Sci. Eng. Technol.*, vol. 11, no. 12, pp. 38–51, 2024, [Online]. Available: www.ijiset.com

[2] Diana D'Abruzzo, "Digital Front Lines A sharpened focus on the risks of, and responses to, hybrid warfare.," Volume 250 from Foreign Policy, FPAnalytics, 2023.

[3] FBI | CISA | MS-ISAC, "#StopRansomware: LockBit 3.0," *Join Cybersecurity Advis.*, 2023.

[4] S. M. Nikola Vidovic, Vladimir M.Cvetkovic, Hatidza Berisa, "Understanding Ransomware Through the Lens of Disaster Risk: Implications for Cybersecurity and Economic Stability," 2025, *International Journal of Disaster Risk Management* •. [Online]. Available: https://internationaljournalofdisasterriskmanagement.com/Vol1/article/view/146/94

[5] M. Hansel and J. Silomon, "Ransomware as a threat to peace and security: understanding and avoiding political worst-case scenarios," *J. Cyber Policy*, vol. 9, no. 2, pp. 159–178, 2024, doi: 10.1080/23738871.2024.2357092.

[6] D. P. Ham, M. Asthi, S. Ari, A. Hakim, and A. Baihaqy, "Analisa Dampak Kebocoran Data Pusat Data Nasional ( Pdn ) Andhika Pratama Adhi Surya M . Asif Nur Fauzi," Vol. 4, No. 156, Pp. 31–37, 2025. doi: https://doi.org/10.57123/wicarana.v3i1.167

[7] M. P. Rayadi, "Fakta-Fakta Brain Cipher: Hacker yang Bobol PDNS 2 di Surabaya Sumber Artikel berjudul " Fakta-Fakta Brain Cipher: Hacker yang Bobol PDNS 2 di Surabaya "," *www.Pikiran-Rakyat.com*, 2024. [Online]. Available: https://www.pikiran-rakyat.com/teknologi/pr-018282233/fakta-fakta-brain-cipher-hacker-yang-bobol-pdns-2-di-surabaya

[8] T. I. Team, "LockBit 3.0 Technical Analysis," 2022.

[9] O. Akinyemi, R. Sulaiman, N. A. preprint arXiv:2308.05565, and undefined 2023, "Analysis of the LockBit 3.0 and its infiltration into Advanced's infrastructure crippling NHS services," *arxiv.orgPaperpile*, vol. 5, no. 1, pp. 24–32, 2024,

[Online]. Available: https://arxiv.org/abs/2308.05565
[10]L. Marlock, “LockBit 3.0 Ransomware: Analysis, Detection, and Mitigation,” SentinelOne Anthology – in-depth analysis of LockBit 3.0’s anti-forensics and detection evasion. [Online]. Available: https://www.sentinelone.com/anthology/lockbit-3-0-lockbit-black/
[11]J. Milenkoski, A., & Walter, “Crimeware Trends: Ransomware Developers Turn to Intermittent Encryption to Evade Detection.,” SentinelOne Labs – documents adoption of intermittent encryption by ransomware groups. [Online]. Available: https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/
[12]J. Bang, J. N. Kim, and S. Lee, “Entropy Sharing in Ransomware: Bypassing Entropy-Based Detection of Cryptographic Operations,” *Sensors*, vol. 24, no. 5, pp. 1–31, 2024, doi: 10.3390/s24051446.
[13]B. P. W. Madanayaka, N. S. A. Dias, A. K. D. D. V Samaranayake, K. V. D. A. U. Karawita, K. Y. Abewardhana, and D. Siriwardana, “A Proactive Approach for Behavior Based Ransomware Detection,” in *2023 5th International Conference on Advancements in Computing (ICAC)*, 2023, pp. 346–351. doi: 10.1109/ICAC60630.2023.10417620.
[14]C. A. Putri *et al.*, “The LockBit 3 . 0 Brain Cipher : Serangan Ransomware terhadap Pusat Data Nasional Indonesia Program Studi Sistem Komputer , Fakultas Teknik Elektro dan Teknologi,” pp. 1–8, 2024.
[15]Y. W. Ghalib *Et Al.*, “Analisis Perkembangan Keamanan Siber Dampak Dari Kebocoran Data Pusat Data Nasional Sementara 2 Surabaya Assessing And Understanding The Current Situation: Analysis Of Cyber Security Developments The Impact Of The Temporary National Data Center Data Leaks 2 Surabaya Oleh,” *Jisco(Journal Informaaon Syst. Compuung) Issn*, Vol. 2, No. June, 2024.
[16]A. Ineza, Y., Jackson, G., Niyonkuru, P., Kevil, J., & Serwadda, “Intermittent File Encryption in Ransomware: Measurement, Modeling, and Detection,” arxiv.org. [Online]. Available: https://arxiv.org/abs/2501.01234
[17]J. Milenkoski, A., & Walter, “Crimeware Trends: Ransomware Developers Turn to Intermittent Encryption to Evade Detection.,” 2025. [Online]. Available: https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/
[18]Y. M. Al-Awadi, A. Baydoun, and H. Ur Rehman, “Can Windows 11 Stop Well-Known Ransomware Variants? An Examination of Its Built-in Security Features,” *Appl. Sci.*, vol. 14, no. 8, 2024, doi: 10.3390/app14083520.
[19]Y. Hou *et al.*, “Preventing Disruption of System Backup against Ransomware Attacks,” *Proc. ACM Softw. Eng.*, vol. 2, no. ISSTA, pp. 229–249, 2025, doi: 10.1145/3728880.
[20]Core Security Labs, “Analysis of CVE-2023-28252 CLFS Vulnerability,” 2023. [Online]. Available: https://www.coresecurity.com/core-labs/articles/analysis-cve-2023-28252-clfs-vulnerability
[21]D. She, Y. Chen, A. Shah, B. Ray, and S. Jana, “Neutaint: Efficient Dynamic Taint Analysis with Neural Networks,” in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 1527–1543. doi: 10.1109/SP40000.2020.00022.
[22]Claire Meyer, “Indonesia Refuses to Pay $8M Ransom in Data Center Cyberattack,” ASIS International. [Online]. Available:

https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2024/june/indonesia-ransomware/
[23]DTrust Team, "Kebocoran Data PDNS: Apa yang Terjadi dan Pelajaran yang Bisa Kita Petik?" [Online]. Available: https://resources.dtrust.co.id/blog/kebocoran-data-pdns-apa-yang-terjadi-dan-pelajaran-yang-bisa-kita-petik/
[24]sentinelone, "Brain Cipher." [Online]. Available: https://www.sentinelone.com/anthology/brain-cipher/
[25]D. Antoniuk, "Indonesia's national data center encrypted with LockBit ransomware variant," 2024. [Online]. Available: https://therecord.media/indonesia-national-data-centre-hacked
[26]M. Syafaruddin, "Brain Cipher Berikan Kunci Enkripsi Ransomware PDNS, Akhiri Drama Serangan Siber," suarasurabaya. [Online]. Available: https://www.suarasurabaya.net/kelanakota/2024/brain-cipher-berikan-kunci-enkripsi-ransomware-pdns-akhiri-drama-serangan-siber/
[27]Antaranews, "Non-state actor behind PDNS 2 cyberattack: Minister," Antara Indonesia News Agancy. [Online]. Available: https://en.antaranews.com/news/317145/non-state-actor-behind-pdns-2-cyberattack-minister
[28]Peris.Ai, "Peris.ai Analysis: Brain Cipher Ransomware Attack on Indonesia's National Data Center."
[29]A. M. Damar, "Kaleidoskop 2024: PDNS 2 Kena Serang Ransomware, Layanan Publik Sempat Lumpuh." [Online]. Available: https://www.liputan6.com/tekno/read/5851302/kaleidoskop-2024-pdns-2-kena-serang-ransomware-layanan-publik-sempat-lumpuh
[30]N. S. Indiraphasa, "Gagal Tangani Serangan Ransomware PDNS, Dirjen Aptika Kominfo Mundur Sumber: https://nu.or.id/nasional/gagal-tangani-serangan-ransomware-pdns-dirjen-aptika-kominfo-mundur-RL25g ___ Download NU Online Super App, aplikasi keislaman terlengkap! https://nu.or."