DAFTAR PUSTAKA

Accenture. (2023). *Cybersecurity trends: Ransomware evolution and enterprise defense*. https://www.accenture.com

Aditya, H., Aminudin, A., & Supriyanto, A. (2024). *Ketahanan Infrastruktur Digital Nasional dalam Menghadapi Ancaman Siber*. Jurnal Ketahanan Siber Indonesia, 5(1), 12–23.

Ahmed, M., Khan, S., & Li, Y. (2024). *AI-based ransomware detection: A comprehensive review. Journal of Cybersecurity and Artificial Intelligence*, 3(2), 88–102. https://doi.org/10.1016/j.jcai.2024.02.003

Alharthi, S., & Sarrab, M. (2021). The impact of *ransomware* on cybersecurity: Mitigation techniques and future trends. *Journal of Cybersecurity and Applications, 20*(3), 15–26.

Almukaynizi, M., Continella, A., Antonakakis, M., & Dagon, D. (2021). *Ransomware payments in the Bitcoin ecosystem. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. https://doi.org/10.1145/3460120.3484741

Any.Run. (2024). *LockBit 3.0 ransomware behavior and sandbox analysis*. Retrieved from https://any.run/malware-trends/lockbit

ASEAN. (2023). *ASEAN Cybersecurity Cooperation Strategy 2023–2027*. https://asean.org

Badan Siber dan Sandi Negara. (2023). *Laporan tahunan insiden siber Indonesia 2023*. https://www.bssn.go.id

Brain Cipher. (2024, Juli 3). *Public statement: Free decryption key for Indonesian PDNS attack*. Retrieved from https://darkwebintel.com/braincipher-release-key

BSSN. (2024). *Rencana Aksi Nasional Keamanan Siber (RAN Kamsiber) 2024–2028*. https://bssn.go.id

BSSN. (2021). Strategi keamanan siber nasional Indonesia. Badan Siber dan Sandi Negara. https://bssn.go.id/strategi-keamanan-siber-nasional/

Chainalysis. (2024). *Crypto crime mid-year update: Ransomware revenue plunges*. https://www.chainalysis.com/blog/crypto-crime-ransomware-2024/

Check Point Research. (2024). *Cyber attack trends: 2024 mid-year report*. Check Point Software Technologies.

CISA. (2024). *Ransomware Threat Report 2023–2024. U.S. Cybersecurity and Infrastructure Security Agency*. https://www.cisa.gov

CNBC Indonesia. (2024, Juni 27). *Kronologi lengkap Pusat Data Nasional diserang hacker, minta Rp 131 M*. https://www.cnbcindonesia.com/tech/20240627171616-37-549973/kronologi-lengkap-pusat-data-nasional-diserang-hacker-minta-rp-131-m

Collier, B., Horgan, S., Jones, R., & Shepherd, L. (2020). The impact of *ransomware* on critical infrastructure: Lessons learned from global incidents. *Computers & Security, 96*(12), 101873.

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches (3rd ed.)*. SAGE Publications.

CSIRT.ID. (2024). *Laporan insiden ransomware LockBit 3.0 pada PDNS*. https://csirt.id/lockbit3-insiden-pdns-juni2024

Cuckoo Sandbox. (n.d.). *Open source automated malware analysis system*. Retrieved from https://cuckoosandbox.org/

Cybersecurity & Infrastructure Security Agency. (2023). *#StopRansomware: LockBit 3.0*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

DPR RI. (2024, Juni 27). *Komisi I DPR bahas serangan ransomware terhadap PDNS bersama Kominfo dan BSSN*. https://www.dpr.go.id/berita/detail/id/4567

Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA)*. https://www.europol.europa.eu/iocta

Europol. (2023). *LockBit ransomware group disrupted in international law enforcement operation*. Retrieved from

https://www.europol.europa.eu/media-press/newsroom/news/lockbit-ransomware-group-disrupted-in-international-law-enforcement-operation

Georgetown University. (2024). *Emerging cyber threats in national critical infrastructure. Center for Security Studies*. https://css.georgetown.edu

Ghidra. (n.d.). *A software reverse engineering (SRE) framework*. Retrieved from https://ghidra-sre.org/

Google Cloud. (2024). *Ransomware protection and containment strategies*. https://cloud.google.com/blog/topics/threat-intelligence/ransomware-protection-and-containment-strategies

Gupta, S., & Tripathi, R. (2021). *Systematic literature review on ransomware detection. International Journal of Cybersecurity Research*, 9(4), 199–215. https://doi.org/10.1016/j.ijcsr.2021.10.007

Hamdani, S. (2024). *Implementasi metode fenomenologi dalam penelitian pendidikan Islam*. *Ta'dib: Jurnal Pendidikan Islam dan Isu-isu Sosial*, 22(1). Retrieved from https://jurnal.iaihnwpancor.ac.id/index.php/tadib/article/download/1560/1013/6876

Hull, G., Li, W., & Chow, K. (2019). *Ransomware deployment methods and analysis. Cybercrime and Security Journal*, 14(2), 45–60.

IBM Security X-Force. (2023). *Threat intelligence index 2023*. https://www.ibm.com/reports/threat-intelligence

IDA Pro. (n.d.). *Interactive Disassembler – Malware reverse engineering tool*. Retrieved from https://hex-rays.com/ida-pro/

ISO/IEC. (2016). *ISO/IEC 27035-1:2016 – Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*. https://www.iso.org/standard/60803.html

Journal of Cybersecurity and Privacy Management. (2023). *Cyber resilience frameworks and their applications in 2023*. https://jcpm.org

Jones, D., Miller, A., & Rogers, T. (2023). *Business continuity in the age of ransomware. Journal of Disaster Risk Reduction*, 39(9), 102141. https://doi.org/10.1016/j.drrr.2023.102141

Kaspersky. (2023). *Indicators of Compromise (IoCs) and ransomware prevention tips*. Retrieved from https://www.kaspersky.com/blog/iocs-guide-ransomware

Kaspersky. (2023). *LockBit 3.0 technical analysis and threat intelligence*. https://securelist.com/lockbit-3-analysis/

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Kebijakan pembangunan pusat data nasional*. https://www.kominfo.go.id

Kementerian Komunikasi dan Informatika (Kominfo). (2024, Juli 4). *Konfirmasi kunci dekripsi Brain Cipher berhasil pulihkan PDNS*. https://kominfo.go.id

Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. (2018). *Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE)*. https://peraturan.bpk.go.id/Details/97319/perpres-no-95-tahun-2018

Kompas Tekno. (2024, Juli 10). *Kronologi serangan ransomware ke PDN dan penanganannya yang tak kunjung usai*. https://tekno.kompas.com/read/2024/07/10/12350077/kronologi-serangan-ransomware-ke-pdn-dan-penanganannya-yang-tak-kunjung-usai

KumparanTech. (2024, Juni 25). *Kronologi server PDNS 2 lumpuh gegara Brain Cipher ransomware*. https://kumparan.com/kumparantech/kronologi-server-pdns-2-lumpuh-gegara-brain-cipher-ransomware-231ExrFZQ5z

Kurniati, A. (2024). *Kajian peran artificial intelligence untuk memperkuat keamanan siber pada infrastruktur informasi vital. MONAS: Jurnal Inovasi Aparatur*, 6(2), 154–165. Retrieved from https://ejournal-bpsdm.jakarta.go.id/index.php/monas/article/download/251/82/

Media Indonesia. (2024, Juli 3). *Kronologi serangan ransomware ke PDNS, mulai dari tebusan USD8 juta hingga kunci dekripsi gratis*. https://mediaindonesia.com/teknologi/682359/kronologi-serangan-ransomware-ke-pdns-mulai-dari-tebusan-usd8-juta-hingga-kunci-dekripsi-gratis

Miller, P., Zhang, T., & Lee, J. (2022). *Ransomware impact on critical infrastructure: A global review. Critical Infrastructure Protection Quarterly*, 5(3), 101–119.

MIT Sloan. (2024). *Cybersecurity Outlook 2024: Cloud and ransomware threats*. https://mitsloan.mit.edu

MITRE ATT&CK. (n.d.). *LockBit ransomware techniques*. Retrieved from https://attack.mitre.org/software/S1053/

MITRE. (2023). *MITRE ATT&CK framework*. https://attack.mitre.org

Morgan, S. (2021). Cybersecurity workforce study 2021: Trends and challenges in the industry. *Cybersecurity Ventures Report*.

Nasir, A., Nurjana, N., Shah, K., Sirodj, R. A., & Afgani, M. W. (2023). *Pendekatan fenomenologi dalam penelitian kualitatif. Innovative: Journal of Social Science Research*, 6(1). Retrieved from https://j-innovative.org/index.php/Innovative/article/view/5224

National Cyber Security Centre. (2023). *LockBit ransomware: Technical details and mitigation advice*. Retrieved from https://www.ncsc.gov.uk/news/lockbit-ransomware-guidance

National Institute of Standards and Technology. (2012). *Computer security incident handling guide (Special Publication 800-61 Rev. 2)*. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). https://www.nist.gov/cyberframework

NIST. (2020). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). National Institute of Standards and Technology.* https://www.nist.gov/cyberframework

Palo Alto Networks Unit 42. (2024). *2024 ransomware threat report*. https://www.paloaltonetworks.com/resources/research/unit42-2024-ransomware-threat-report

Palo Alto Networks Unit 42. (2023). *LockBit 3.0 ransomware technical analysis*. Retrieved from https://unit42.paloaltonetworks.com/lockbit-3-0-ransomware/

Patel, R. (2024). *Disaster recovery and business continuity in a ransomware world. Cyber Risk Management Review*, 12(1), 45–58.

Perez, A., & Collins, M. (2024). *Cybersecurity in the Age of Ransomware: Lessons from Global Attacks*. *Journal of Cyber Defense*, 12(1), 33-48.

Perez, A., & Li, C. (2024). *Impact of ransomware on cloud-based data centers. Journal of Cloud Computing and Security*, 4(1), 25–41.

Ransomware Task Force. (2021). *Combating ransomware: A comprehensive framework for action*. *Institute for Security and Technology.* https://securityandtechnology.org/ransomwaretaskforce/report/

Setiawan, A. B. (2015). *Kajian strategi pengamanan infrastruktur sumber daya informasi kritis*. *Buletin Pos dan Telekomunikasi*, 13(2), 45–54. Retrieved from https://bpostel.kominfo.go.id/index.php/bpostel/article/view/113/130

Sikorski, M., & Honig, A. (2021). *Practical malware analysis: The hands-on guide to dissecting malicious software*. No Starch Press.

Smith, J. A., Flowers, P., & Larkin, M. (2009). *Interpretative phenomenological analysis: Theory, method and research*. SAGE Publications.

Smith, J., Tan, L., & Rahman, A. (2023). *The Rise of Ransomware: Global Trends and Strategic Responses*. *Cybersecurity Review*, 9(3), 101–119.

Smith, R., Walker, N., & Chang, A. (2020). *Dynamic analysis of ransomware attacks. Journal of Malware Studies*, 7(3), 34–50.

Sutomo, S., et al. (2025). *Pengembangan model strategi pertahanan siber berbasis manajemen risiko untuk melindungi infrastruktur informasi vital nasional. Temali: Jurnal Pembangunan Sosial*, 8(1), 29–40. Retrieved from https://journal.uinsgd.ac.id/index.php/temali/article/download/38690/pdf/121909

Swascan. (2023, August 21). *LockBit 3.0 ransomware analysis: A deep dive.* https://www.swascan.com/lockbit-3-0-ransomware-analysis/

Symantec Enterprise Blogs. (2022). *LockBit 3.0: The latest version of the prolific ransomware operation*. Retrieved from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockbit-3-ransomware

TRM Labs. (2024). *Ransomware in 2024: Latest trends, mounting threats, and the government response*. https://www.trmlabs.com/post/ransomware-in-2024-latest-trends-mounting-threats-and-the-government-response

Unit 42. (2023). *Ransomware threat report: LockBit and beyond. Palo Alto Networks*. https://unit42.paloaltonetworks.com

VMware Carbon Black. (2022). *Threat Analysis Unit: LockBit 3.0 – Evolution of a notorious ransomware family*. https://www.vmware.com/resources/security/lockbit-3-analysis.html

World Economic Forum. (2022). *Cyber resilience in the digital economy*. https://www.weforum.org

World Economic Forum. (2023). *Global cybersecurity outlook 2023*. https://www.weforum.org/reports/global-cybersecurity-outlook-2023/

World Economic Forum. (2022). *The global risks report: Digital resilience in critical systems*

Yohanes, M. (2023). *Analisis serangan Lockbit 3.0: Teknik dan dampaknya terhadap infrastruktur vital*. Retrieved from https://cybersecurity.id/article/lockbit3-yohanes

Zhou, L., Tanaka, H., & Martinez, R. (2022). *Ransomware prevention and mitigation techniques. Journal of Information Technology & Security*, 17(4), 98–111. https://doi.org/10.1016/j.jits.2022.04.005

Zimba, A., & Chishimba, S. (2020). Digital forensiks in *ransomware* attacks: A case study of *Lockbit* 2.0 and *Lockbit* 3.0. *International Journal of Digital* Forensik*s & Cybersecurity, 9*(1), 1–12.