FMDB *Transactions on Sustainable Intelligent Networks*

Analysis of LockBit 3.0 and its Infiltration into Advanced's Infrastructure, Crippling NHS Services

Oladipupo Akinyemi[1,*], Rejwan Sulaiman[2], Nasr Abosata[3]

[1,2,3]Faculty of Engineering and Environment, Northumbria University, Middlesex Street, London, United Kingdom.
oladipupo.akinyemi@nortumbria.ac.uk[1], rejwan.sulaiman@northumbria.ac.uk[2], nasr.abosata@northumbria.ac.uk[3]

Abstract: The most dangerous ransomware variation in recent years is LockBit 3.0, which demands $8 million without regard for the ransom from a victim. According to Trend, ransomware has evolved through micro simulations of healthcare, education, and technology to become adaptable and evasive, infiltrating the Advanced Computer Software group and threatening governments and organisations across oil and gas, manufacturing, transportation, and other sectors. Threat actors have historically targeted lock industries and have proven they are in for the long haul. Kaspersky also claims that ransomware attacks, prevention, encryption detection, decryption, and the rise in remote working could hinder data recovery, making it pointless to rule out this type of attack in less tech-savvy industries, where the attack mode is rarely examined. This paper examines LockBit and its objectives. 3.0 assault methods with context illustrations. Lock-on Advanced Computer Software group, including the NHS, has changed over time. An evolutionary variant that developed from a key client of the business, and the disabling of its services for hours alongside 15 other clients during the attack, illustrate the terrible disruption such events can wreak on critical organisations. Researchers noticed that LockBit upgrades by releasing fresh versions are a bid to keep the malware highly efficient by staying ahead of improving safeguards.

Keywords: Computer Software; Encryption Detection; LockBit Threat; Cyber Insurance; Attack Techniques; Detection Systems; Evolutionary Variant; Remote Work Vulnerabilities.

Received on: 06/11/2024, **Revised on:** 14/01/2025, **Accepted on:** 14/02/2025, **Published on:** 05/09/2025

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSIN

DOI: https://doi.org/10.69888/FTSIN.2025.000535

Cite as: O. Akinyemi, R. Sulaiman, and N. Abosata, "Analysis of LockBit 3.0 and its Infiltration into Advanced's Infrastructure, Crippling NHS Services," *FMDB Transactions on Sustainable Intelligent Networks*, vol. 2, no. 3, pp. 129–136, 2025.

1. Introduction

Since its inception, LockBit, a ransomware-as-a-service (RaaS), has proven to be a large-scale threat [13]. Discovered in 2019 and initially dubbed the ".abcd virus" (coined from the victim's encrypted file extension), the ransomware is linked to a third of ransomware attacks recorded since the second half of 2022. Although Blackberry [3] depicts LockBit targets as small-to-medium-sized organisations due to the ridiculously cheap ransom demanded when compared to an average ransomware payment, Abrams [4] claims the .abcd extension, then the. LockBit extension, and then the LockBit 2.0 version [1]. The latest variant – LockBit 3.0, also known as LockBit Black - is the most adaptable and evasive of the versions [6]. SOCRadar [2] reports that, although LockBit 3.0 is known to target Windows, Linux, and VMware ESXi servers, new versions capable of

[*] Corresponding author.

targeting macOS, MIPS, ARM, FreeBSD, and SPARC servers have been identified recently [18]. It is therefore important that organisations strengthen their defences, as there may be a proportionate increase in LockBit attacks as more target devices become penetrable. Amazingly, the assumption that Cyber Insurance could help mitigate ransomware attacks is somewhat plausible. Khodjibaev et al. [7] recall how a LockBit operator insinuated that an attack on a cyber-insured firm would guarantee a successful payment. Also, a member of the REvil group once referred to cyber-insurance companies as "one of the tastiest morsels" and explained that hacking them was a resourceful way to conduct reconnaissance before attacking clients [8]. It is therefore important that organisations become more intentional about the secure storage of their data [13].

This paper examines the LockBit 3.0 ransomware, using the attack on an Advanced software provider that crippled the UK NHS 111 services as a case study. Understanding that Advanced issued a statement confirming that 16 of its Staff-Plan and Caresys Customer companies were affected by the ransomware attack, this paper analyses the attack and proposes futuristic countermeasures [9]. However, it is important to note that conclusions from previous studies on encryption, decryption, recovery, etc., rarely accounted for LockBit's rapid version transitions, thereby sometimes rendering their proposed solutions premature and unhelpful [14]; [17]. Therefore, having a broad understanding of how the attack is carried out is likely to be beneficial as patterns are less susceptible to change [16]. To learn from the attack to bolster the knowledge required to administer countermeasures, relevant journals, research papers, government publications, and online articles on recent ransomware attacks were reviewed for insights [15].

2. Attack Analysis

Conventionally, ransomware threat actors require access to the victim's infrastructure. In the case of LockBit, initial access could be via Remote Desktop Protocol (RDP) exploitation, the abuse of valid accounts, phishing campaigns, the exploitation of public-facing applications, or drive-by compromise [6]. The attack on Advanced was reported to have been initiated using legitimate third-party credentials, suggesting either the abuse of valid accounts or a successful phishing campaign. Furthermore, Advanced stated that in the initial phase of the attack, the attacker moved laterally in the health and care environment and escalated privileges, allowing reconnaissance and the deployment of encryption malware [10]. Cybersecurity and Infrastructure Security Agency [6] claims that privilege escalation could entail gathering system information such as hostname and domain information, stopping services, executing commands, enabling automatic logon for persistent access, and deleting log files, shadow copies, and files in the recycle bin. Although there are several other vulnerabilities the attacker could exploit, for example, Microsoft research identified two vulnerabilities in PaperCut's print management software that, when exploited, allowed LockBit attackers to install remote management software [11]. Understanding that PaperCut's software is widely used across industries, including healthcare, exploitation of these vulnerabilities could have created an avenue for attackers to move laterally through systems, collect information, and launch secondary attacks.

Lateral movement within a target network is eased by using either a predetermined list of credentials hardcoded during compilation or a local account with escalated privileges that has already been compromised. Once compiled, features that may also allow it to spread via Group Policy Objects and PsExec are activated using the Server Message Block (SMB) protocol [6]. The goal of this infiltration is to ensure that recovery is almost impossible without the attacker's assistance. Common to ransomware attacks, information theft is considered vital before encryption. Advanced claimed the attackers were able to steal some information before encryption [9]. Newman [11] explains that the motive behind such theft is to threaten victims by publicly exposing the information if ransom isn't paid. He further explained that some attackers fancy double extortion, i.e., files are encrypted in two layers, each requiring a ransom for decryption. Castaño et al. [5] claim tools such as MEGA, FreeFileSync, and StealBit – exclusive to LockBit – are used to exfiltrate stolen files. Given that Advanced is a British organisation, its systems will most likely have English set as the language. Lakshmanan [12] claims that the ransomware was programmed to infect only systems configured with languages outside the exclusion list, including Romanian (Moldova), Arabic (Syria), and Tatar (Russia). Therefore, the attack program halts when any of these languages is detected. Once the network is ready for LockBit to operate, the ransomware will begin spreading across any accessible devices.

LockBit can achieve this with minimal requirements. With a single device that has elevated privileges, it can send commands to other devices on the network to download and execute ransomware [1]. The encryption function encrypts all system files, essentially" locking" them, making them inaccessible to the victim, ensuring only a custom decryption key created by LockBit's proprietary decryption tool can create access. Although Advanced does not publicly provide precise details of the attack, it states that such information would be provided only upon request. The usual trajectory for LockBit 3.0 attackers after encryption is to drop ransom notes named "<Ransomware ID >.README.txt", and change the host's icon and wallpaper to the attacker's customised images [6]. Furthermore, depending on options set at compilation time, LockBit 3.0 may choose to delete itself and/or any updates made. LockBit affiliates use multiple freeware and open-source tools in their attacks. These tools have been used for various activities, including network reconnaissance, remote access and tunnelling, credential dumping, and file exfiltration. The Cybersecurity and Infrastructure Security Agency [6] claims that PowerShell and Batch scripts are common in most attacks, which focus on system discovery, reconnaissance, password and credential hunting, and privilege escalation. Also, signs of professional penetration testing tools such as Metasploit and Cobalt Strike have been identified (Table 1).

Table 1: LockBit ransomware attack flow and technical analysis

Attack Phase	**Description of Attacker Activity**	**Techniques / Tools Involved**	**Evidence from Advanced / Reports**	**Reference**
Initial Access	Attackers gained entry using legitimate third-party credentials, indicating either account abuse or phishing.	RDP exploitation, phishing, valid account abuse, public-facing application exploitation	Advanced confirmed use of legitimate credentials	[6]; [10]
Privilege Escalation	Elevated privileges were obtained to enable deeper system control and reconnaissance.	Access token manipulation, service stopping, command execution, and auto-logon enabling.	CISA reports privilege escalation behaviours	[6]
Lateral Movement	Attackers moved across healthcare network environments to identify targets and spread malware.	SMB, PsExec, Group Policy Objects, credential reuse	Advanced reported lateral movement before encryption	[6]
Vulnerability Exploitation	Exploitation of third-party software vulnerabilities enabled further access and persistence.	PaperCut print management vulnerabilities, remote management tools	Microsoft identified exploited PaperCut flaws	[11]
Discovery and Reconnaissance	Systems, domains, and network shares were enumerated to identify valuable assets.	PowerShell, batch scripts, Metasploit, Cobalt Strike	CISA observed reconnaissance tooling	[6]
Data Exfiltration	Sensitive information was stolen before encryption, enabling double extortion.	MEGA, FreeFileSync, StealBit (LockBit-exclusive)	Advanced confirmed data theft	[5]; [9]; [12]
Encryption and Impact	Files were encrypted using LockBit's proprietary encryption, rendering systems unusable.	Custom encryption engine, ransomware payload	LockBit 3.0 behaviour observed	[1]; [6]
Ransom and Post-Attack Actions	Ransom notes dropped, system visuals modified, and malware self-deleted in some cases.	README ransom notes, wallpaper changes, self-deletion	Standard LockBit 3.0 tactics	[6]

Figure 1 shows the entire process of a LockBit ransomware attack, from gaining access to paying the ransom and doing things afterwards. Figure 1 shows key steps that mirror the enemy's tactics, such as privilege escalation, lateral movement, vulnerability exploitation, data exfiltration, and encryption. Figure 1 shows how this visual depiction puts together technical tactics, attacker goals, and forensic evidence into a systematic attack path.

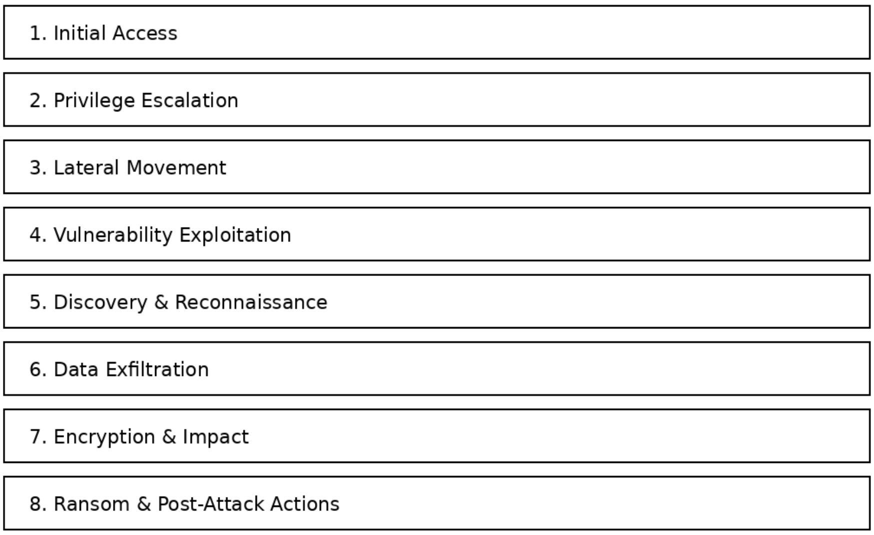


Figure 1: Lifecycle of a LockBit ransomware attack

2.1. Attack Narration

Even though the post-attack information provided by Advanced was superficial, the few details extracted will be used to connect the dots and summarise the attack:

- Social engineering was deployed.
- Third-party credentials stolen.
- Stolen credentials were used to access the management system, bypassing authentication errors because the hashes matched.

Table 2 provides insight into the MITRE tactics the Lockbit 3.0 ransomware may have used against advanced systems.

Table 2: Mitre tactics and techniques

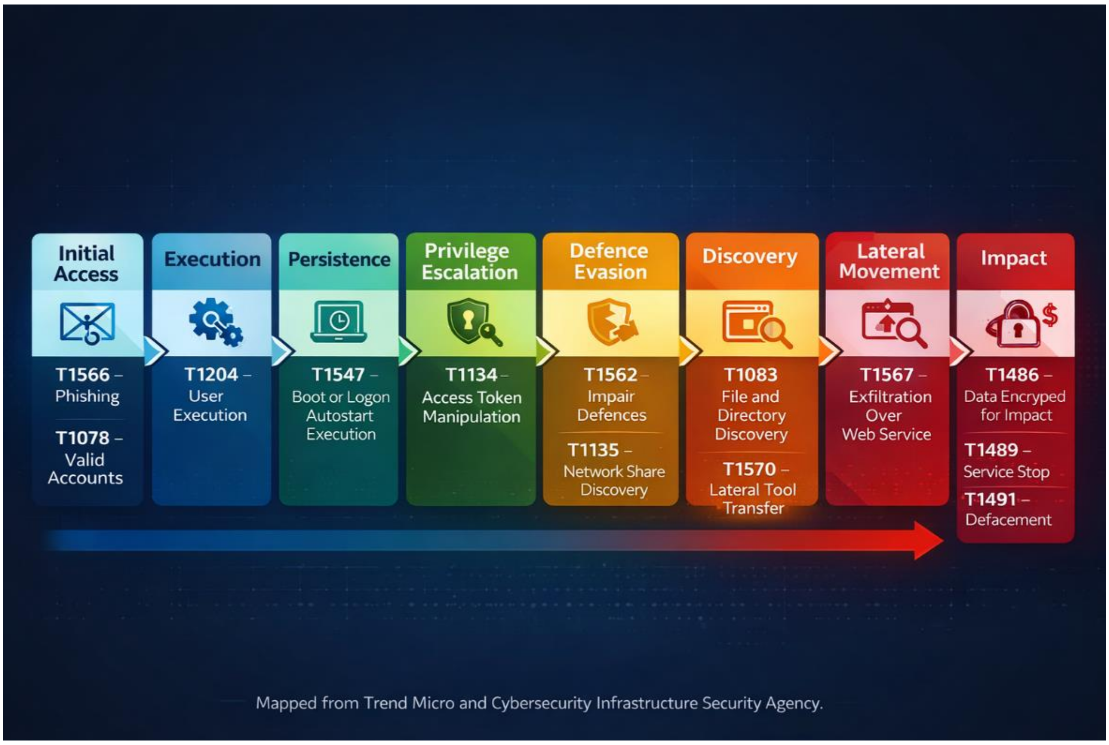
Initial Access	Execution	Persistence	Privilege Escalation	Defence Evasion	Discovery	Lateral Movement	Exfiltration	Impact
T1566 – Phishing	T1204 – User Execution	T1547 – Boot or Logon Autostart Execution	T1134 – Access Token Manipulation	T1562 – Impair Defences	T1083 – File and Directory Discovery	T1570 – Lateral Tool Transfer	T1567 – Exfiltration Over Web Service	T1486 – Data Encrypted for Impact
T1078 – Valid Accounts					T1135 – Network Share Discovery			T1489 – Service Stop
								T1491 – Defacement

a. *Mapped from Trend Micro and Cybersecurity Infrastructure Security Agency.*

- Group policy created to turn off security products, e.g., Windows Defender.
- Management system leveraged and LockBit executed via PowerShell Empire.
- Further credential theft using Mimikatz.
- Using the management system, privileges were escalated to enable reconnaissance and facilitate the deployment of encryption malware.
- Enumeration using network and port scanners is performed to locate domain controllers or Active Directory, as they are often viable targets for deploying ransomware that encrypts the network.
- Lateral movement commenced by self-propagation via SMB protocol using obtained credentials and Group policies.

- Exfiltration occurred with some files stolen and uploaded to cloud storage.
- Advanced’s health and care environment systems were infected, and files were encrypted.
- Ransom notes created, icons and wallpapers changed to notify the victim.

Figure 2 shows how a cyber-attack moves through the main parts of the MITRE ATT&CK framework, from initial access and execution to exfiltration and the end state. It shows how adversaries navigate a system by visually mapping representative ATT&CK tactics to each step. Figure 2 clearly shows this end-to-end attack flow.


Initial Access
T1566 – Phishing
T1078 – Valid Accounts
Execution
T1204 – User Execution
Persistence
T1547 – Boot or Logon Autostart Execution
Privilege Escalation
T1134 – Access Token Manipulation
Defence Evasion
T1562 – Impair Defences
T1135 – Network Share Discovery
Discovery
T1083 File and Directory Discovery
T1570 – Lateral Tool Transfer
Lateral Movement
T1567 – Exfiltration Over Web Service
Impact
T1486 – Data Encrypted for Impact
T1489 – Service Stop
T1491 – Defacement

Mapped from Trend Micro and Cybersecurity Infrastructure Security Agency.

Figure 2: MITRE ATT and CK–based cyber intrusion lifecycle and technique mapping

3. Countermeasures

Arguably one of the biggest threats to individuals and organisations globally, several approaches to detect and prevent ransomware have been identified. However, Mclntosh et al. [13] claim the inability of many anti-ransomware studies to account for the evolution of ransomware from executable files encrypting victim files, to the inclusion of fileless command scripts, information exfiltration, and a human-operated form, could be the reason some recent measures are futile. Although Irwin [15] pins successful ransomware attacks on victim illiteracy, it is important to note that user awareness is only one of the minimum practices required. There are no elementary solutions to protect an organisation from ransomware totally. Young [17] explains that preventing a ransomware attack requires adopting a layered approach using a defence-in-depth methodology, which involves implementing various measures such as providing regular training to users, filtering emails for suspicious content, using virus detection software, configuring firewalls, strengthening edge security, monitoring activities, and employing additional techniques depending on the available budget, resources, and expertise. Regarding LockBit 3.0, the Cross-Sector Cybersecurity Performance Goals (CPGs) prepared by CISA and NIST recommend the following practices and protections for organisations (Table 3).

Table 3: Recommended countermeasures for mitigating LockBit 3.0 ransomware attacks

Security Domain	Countermeasure	Description / Purpose
Data Protection and Recovery	Offline and isolated backups	Maintain multiple encrypted, immutable copies of critical data in a physically isolated, secure, offline environment to enable recovery after ransomware incidents.

Identity and Access Management	NIST-compliant password policies	Enforce strong password standards to reduce the risk of credential compromise and unauthorised access.
Identity and Access Management	Phishing-resistant multifactor authentication	Implement MFA mechanisms resistant to phishing attacks to strengthen authentication security.
System and Software Security	Regular patch management	Continuously update operating systems, applications, and firmware to eliminate exploitable vulnerabilities.
Network Security	Network segmentation	Divide networks into isolated segments to restrict lateral movement and limit ransomware propagation.
Monitoring and Detection	Comprehensive network logging	Log and analyse all network traffic, including lateral movement, to detect anomalies and support incident investigation.
Endpoint Protection	Antivirus and real-time threat detection	Deploy antivirus solutions with real-time scanning and regular updates across all hosts.
Directory and Account Security	Active Directory monitoring	Continuously monitor servers, domain controllers, and Active Directory for unauthorised accounts or misuse of privileges.
Network Hardening	Disable unused ports	Reduce the attack surface by turning off unnecessary and unused network ports.
Email Security	External email tagging	Tag emails received from external sources to increase user awareness of potential phishing attempts.
Email Security	Disable email hyperlinks	Prevent users from directly clicking hyperlinks in emails to reduce phishing-related infections.
Privilege Management	Restrict command-line and scripting permissions.	Limit access to scripting and command-line tools to prevent privilege escalation and lateral movement.
Backup Security	Encrypted and immutable backups	Ensure backups are encrypted, immutable, and include all proprietary organisational data.
Security Validation	Control testing against MITRE ATTandCK	Regularly test implemented controls and validate their effectiveness using mapped MITRE ATTandCK techniques.

- Establish and enforce a recovery strategy that includes preserving multiple copies of sensitive data in a physically isolated, well-protected, offline facility.
- Comply with NIST password policy standards.
- Require phishing-resistant multifactor authentication.
- Regularly patch the operating system, software, and firmware.
- Segment networks to curb ransomware spread.
- Log and report all network traffic, including lateral movement activity, to identify, detect, and investigate abnormalities.
- Install antivirus software on all hosts and ensure real-time detection and regular updates are enabled.
- Monitor servers, domain controllers, and Active Directory for unauthorised accounts.
- Disable unused ports.
- Tag emails received from outside sources with an email banner.
- Disable hyperlinks in emails received.
- Restrict command-line and scripting activities permissions to avoid lateral movement or privilege escalation.
- Ensure backup data is encrypted, contains all organisations' proprietary data, and is immutable.

Additionally, regular testing of existing controls, assessing their performance against the MITRE techniques mapped out, is recommended (Figure 3).

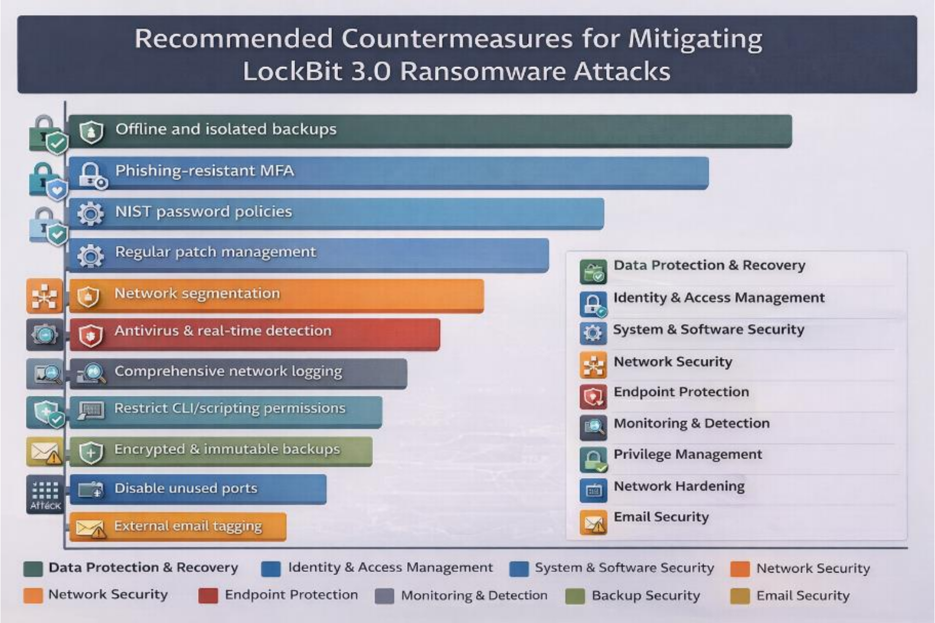

Recommended Countermeasures for Mitigating LockBit 3.0 Ransomware Attacks
Offline and isolated backups
Phishing-resistant MFA
NIST password policies
Regular patch management
Network segmentation
Antivirus & real-time detection
Comprehensive network logging
Restrict CLI/scripting permissions
Encrypted & immutable backups
Disable unused ports
External email tagging
Attack
Data Protection & Recovery
Identity & Access Management
System & Software Security
Network Security
Endpoint Protection
Monitoring & Detection
Privilege Management
Network Hardening
Email Security
Data Protection & Recovery
Identity & Access Management
System & Software Security
Network Security
Network Security
Endpoint Protection
Monitoring & Detection
Backup Security
Email Security

Figure 3: LockBit 3.0 mitigation strategies hierarchy

4. Conclusion

In this paper, the recent LockBit variant 3.0 was analysed in the context of the attack on the Advanced Computer Software group and its customers, one of which was the UK NHS. The objective was to establish a comprehensive understanding of how Lockbit 3.0 ransomware infiltrated network infrastructure, which could aid future prevention of the malware and its variants by providing insights into its attack patterns and recommendations for countermeasures. This paper establishes the extent of LockBit 3.0's influence in the ransomware market. It was found that LockBit's evolution over time has enhanced its adaptation to its target environment and evasion of defensive measures, making its perpetrators the biggest on the scene. Based on reports, the paper illustrated, through a LockBit attack scenario on Advanced, that credentials obtained through social engineering can create pathways for attackers to move laterally within an infrastructure, escalate privileges, exfiltrate data, and encrypt it. However, it is important to acknowledge the limitations of this study. While the analysis may seem agreeable, the lack of direct intel from Advanced Computer Software Group limited the information gathered for this study to third-party sources, thereby impeding accuracy. In the end, this study shows that there is no straightforward countermeasure against ransomware and specifically highlights recommendations to mitigate LockBit 3.0 attacks. The attack narrative and analysis have provided valuable insights into prevention and detection. However, given the rising sophistication of ransomware attacks, it is crucial to regularly evaluate the effectiveness of detection and preventive measures to identify any shortcomings that need to be addressed.

Acknowledgement: The authors would like to express their sincere gratitude to Northumbria University for providing a supportive academic environment and essential resources that facilitated the successful completion of this research.

Data Availability Statement: The data supporting the findings of this study are not publicly available due to ethical and confidentiality considerations; however, they may be obtained from the corresponding authors upon reasonable request. Access to the data will be granted in accordance with institutional policies and ethical guidelines to support transparency and reproducibility.

Funding Statement: This research and the preparation of the manuscript were carried out without any external financial support. No funding was received from public, commercial, or non-profit funding agencies.

Conflicts of Interest Statement: The author declares no financial, professional, or personal conflicts of interest that could have influenced the conduct or outcomes of this research. This work constitutes an original scholarly contribution, and all sources of information and prior studies have been properly cited and acknowledged.

Ethics and Consent Statement: This study was conducted in compliance with established ethical standards and institutional research guidelines. Informed consent was obtained from all participants before their participation, and appropriate safeguards were implemented to ensure confidentiality, anonymity, and the protection of participant data throughout the research process.

References

1. Kaspersky, “LockBit ransomware - What you need to know,” *Kaspersky*, 2023. Available: https://me-en.kaspersky.com/resource-center/threats/lockbit-ransomware [Accessed by 14/09/2024].
2. SOCRadar, “Dark Web Profile: LockBit 3.0 Ransomware,” *SOCRadar*, 2023. Available: https://socradar.io/blog/dark-web-profile-lockbit-3-0-ransomware/ [Accessed by 27/09/2024].
3. Blackberry, “How LockBit 2.0 Ransomware Works and Indicators of Compromise,” *Blackberry*, 2021. Available: https://blogs.blackberry.com/en/2021/08/threat-spotlight-lockbit-2-0-ransomware-takes-on-top-consulting-firm [Accessed by 27/09/2024].
4. L. Abrams, “LockBit ransomware blames Entrust for DDoS attacks on leak sites,” *BleepingComputer*, 2022. Available: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-blames-entrust-for-ddos-attacks-on-leak-sites/ [Accessed by 22/09/2024].
5. F. Castaño, C. Patsakis, F. Zola, and F. Casino, “Inside LockBit: Technical, behavioral, and financial anatomy of a ransomware empire,” *arXiv preprint, arXiv:2511.06429*, 2025. Available: https://arxiv.org/pdf/2511.06429 [Accessed by 11/07/2025].
6. Cybersecurity and Infrastructure Security Agency, “StopRansomware: LockBit 3.0,” *CISA.gov*, 2023. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a [Accessed by 16/09/2024].
7. A. Khodjibaev, D. Korzhevin, and K. McKay, “Interview with a LockBit ransomware Operator New York,” *Talos Blog*, 2021. Available: https://blog.talosintelligence.com/interview-with-lockbit-ransomware/ [Accessed by 02/09/2024].
8. G. Mott, S. Turner, J. R. C. Nurse, J. MacColl, J. Sullivan, A. Cartwright, and E. Cartwright, “Between a rock and a hard(ening) place: Cyber insurance in the ransomware era,” *Computers and Security*, vol. 128, no. 5, p. 103162, 2023.
9. The Stack, “Advanced confirms attack was LockBit 3.0 ransomware, legitimate creds used,” *the stack.technology*, 2022. Available: https://www.thestack.technology/advanced-data-breach-credentials-ransomware-post-incident-summar/ [Accessed by 13/09/2024].
10. C. Glover, “PaperCut vulnerabilities exploited using LockBit and Cl0p ransomware – Microsoft,” *Tech Monitor*, 2023. Available: https://www.techmonitor.ai/technology/cybersecurity/papercut-vulnerability-lockbit-clop-microsoft-ransomware [Accessed by 28/09/2024].
11. L. H. Newman, “Ransomware’s Dangerous New Trick Is Double-Encrypting Your Data,” *Wired*, 2021. Available: https://www.wired.com/story/ransomware-double-encryption/ [Accessed by 17/09/2024].
12. R. Lakshmanan, “LockBit 3.0 Ransomware: Inside the Cyberthreat That’s Costing Millions,” *The Hacker News*, 2023. Available: https://thehackernews.com/2023/03/lockbit-30-ransomware-inside.html [Accessed by 18/09/2024].
13. T. Mclntosh, A. S. M. Kayes, P. C. Yi-Ping, A. Ng, and P. Watters, “Applying staged event-driven access control to combat ransomware,” *Computers and Security*, vol. 128, no. 5, p. 103160, 2023.
14. V. R. Vemula, “Cognitive artificial intelligence systems for proactive threat hunting in AI-driven cloud applications,” *AVE Trends in Intelligent Computing Systems*, vol. 1, no. 3, pp. 173–183, 2024.
15. L. Irwin, “Lack of education is the leading cause of successful ransomware attacks,” *itgovernance.co.uk*, 2019. Available: https://www.itgovernance.co.uk/blog/lack-of-education-is-the-leading-cause-of-successful-ransomware-attacks [Accessed by 26/09/2024].
16. A. R. Pothu, “Behavioural analysis of end-users for enhancing cybersecurity awareness and prevention,” *AVE Trends in Intelligent Computer Letters*, vol. 1, no. 1, pp. 31–40, 2025.
17. S. Young, “When ransomware strikes, what’s your recovery plan?” *Network Security*, vol. 2021, no. 7, pp. 16-19, 2021.
18. A. R. P. Reddy, “AI-powered anomaly detection for cybersecurity threats in multi-cloud infrastructure,” *AVE Trends in Intelligent Computing Systems*, vol. 2, no. 2, pp. 77–86, 2025.