JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

LockBit 3.0: An Analysis of Its Development, Techniques, and Mitigation Strategies

Keshav, Prof. Neetha S S, Dr. Shyam R.

Student, Jain (Deemed-to-Be) University, Bangalore.

Assistant Professor, Jain (Deemed-to-Be) University, Bangalore.

Assistant Professor, Jain (Deemed-to-Be) University, Bangalore.

Abstract:

LockBit ransomware has emerged as a significant and persistent threat in the cybersecurity industry. The efficacy of its techniques and business structure has made it extremely appealing to cybercriminals, raising its level of danger and influence in recent times. The key objective of this study is to thoroughly investigate the execution methods of this extremely skilled ransomware and provide effective solutions for the public, companies, and critical infrastructure to protect themselves against it. The objective of this research is to provide readers with a comprehensive comprehension of ransomware, its ramifications, and the precautionary measures that can be implemented to safeguard against its impacts.

I. INTRODUCTION

Lockbit ransomware has emerged as a highly detrimental and enduring threat within the expansive and intricate realm of cybersecurity. This malware is specifically programmed to impede access to a computer system until a specified amount of money, usually in the form of cryptocurrency, is transferred to the individual responsible for the attack. Ransomware attacks have undergone significant advancements in complexity, sophistication, and impact in recent years.

Lockbit ransomware has evolved from being transmitted through physical storage devices to advanced phishing campaigns and exploits. The introduction of the ransomware-as-a-service (RaaS) model has further transformed the landscape of potential threats. Within this framework, ransomware developers provide their malicious software as a service to less-informed criminals, who subsequently execute incidents and distribute their earnings to the developers. As a result, ransomware attacks have become increasingly common and profitable.

LockBit 2.0 is a variant of malware that encrypts data and demands a ransom. It primarily targets organizations but claims to spare healthcare, education, and other critical sectors. However, there have been instances where individuals associated with these sectors have disregarded these instructions.

Ransomware poses a substantial threat to critical infrastructure, businesses, and individual users alike. Crucial sectors such as finance, insurance, government operations, and critical infrastructure have been specifically targeted by highly destructive ransomware attacks. In 2021, US banks and financial institutions processed approximately $1.2 billion in ransomware payments. Although the financial expenses associated with these attacks can be extremely high, the harm they cause to business operations and reputations can be even more detrimental.

LockBit has gained notoriety as an exceptionally prolific ransomware threat among the various types of ransomware. LockBit ransomware is an autonomous cryptographic malware that restricts user entry to computer systems and requests a payment in exchange for decryption. Its main focus is on enterprises and government organizations, presenting risks such as operational disruption, extortion, data theft, and blackmail. LockBit functions as a ransomware-as-a-service (RaaS) platform, where interested individuals pay a deposit to access customized attacks for hire and earn profits through an affiliate system.

LockBit has perpetrated numerous prominent attacks on organizations worldwide. The operations of this entity are not constrained by any specific geographic boundaries, as it has targeted numerous organizations across multiple countries, such as the United States, China, India, Indonesia, Ukraine, and various European nations. Curiously, it appears to refrain from targeting systems in Russia or any other countries in the Commonwealth of Independent States.

This review paper seeks to provide a comprehensive analysis of the functioning of LockBit ransomware, its consequences, and the strategies that can be employed to minimize its impact. The primary objective of this review paper is to investigate the operational mechanisms of LockBit ransomware and provide effective strategies for individuals, businesses, and critical infrastructure to safeguard against it. Through the examination of this inquiry, our objective is to elucidate the mechanisms of this highly productive ransomware and offer valuable perspectives on how to reduce its risks.

II. LITERATURE REVIEW

The LockBit ransomware, alternatively referred to as the ".abcd virus" due to the appended file extension it applies to the encrypted files, was initially detected in September 2019. The system functions based on a RaaS (ransomware-as-a-service) framework, in which the affiliates who obtain licenses distribute the ransom payments in collaboration with the LockBit developers.

The second iteration of LockBit, known as version 2.0, was launched in June 2021, and it was implicated in cyber-attacks in regions such as Chile, Taiwan, and the UK. This updated version brought with it the implementation of the double extortion method and the capability for automatic encryption across Windows domains. By October 2021, LockBit had expanded its scope to include Linux servers, specifically targeting ESXi servers.

LockBit selects its targets meticulously, taking into consideration their financial capacity and the potential influence they can exert on their respective organizations. The ransomware's effective strategies and commercial framework have rendered it attractive to cybercriminals, heightening its peril and impact in the realm of cybersecurity.

LockBit gains initial entry into the target networks primarily through acquired access, unaddressed vulnerabilities, insider collaboration, or zero-day exploits. Upon gaining access, it employs a software tool known as "StealBit" to encrypt the files, rendering them inaccessible. This tool possesses high speed and robustness, and it has the capability to propagate to other devices within the network automatically, rendering it difficult to halt instantaneously.

LockBit has been involved in numerous significant cyber incidents, causing severe damage to the targeted organizations and frequently resulting in data breaches, financial losses, and operational disruptions. Notable targets of LockBit attacks include Foxconn, a prominent tech manufacturer; Advanced, a vendor for the NHS; Accenture, a major IT company; and Continental, a German auto parts company.

In the first quarter of 2022, LockBit constituted 15% of ransomware attacks, ranking second after Conti, which accounted for 16%. LockBit accounted for 40% of the ransomware attacks by May of that year. While the overall number of ransomware incidents has declined in recent months, it is probable that LockBit's proportion will rise.

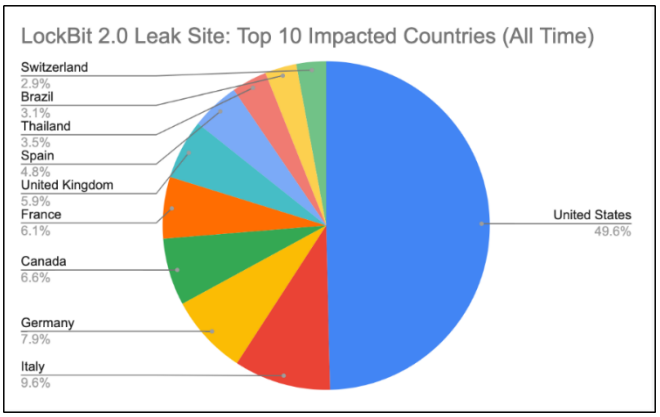


fig. 1(a)

As illustrated in Figure 1(a), the United States emerged as the country with the highest level of impact, representing approximately 49.6% of all impacts. Italy was ranked second in terms of the magnitude of its impact, representing 9.6% of the overall impacts. Germany was ranked third in terms of impact, contributing 7.9% to the overall impacts. Canada and France were significantly affected, accounting for 6.6% and 6.1% of the overall impacts, respectively. The United Kingdom represented 5.9% of the impacts. Spain accounted for 4.8% of the impacts, whereas Thailand represented 3.5% of the total impacts. Brazil accounted for 3.1% of the impacts. Switzerland had the lowest impact among the top 10, accounting for only 2.9% of the total impacts.

Each country's segment in the pie chart is color-coded, corresponding to its percentage impact from the leak site. The chart provides a clear visual representation of the countries most affected by the LockBit 2.0 leak site.

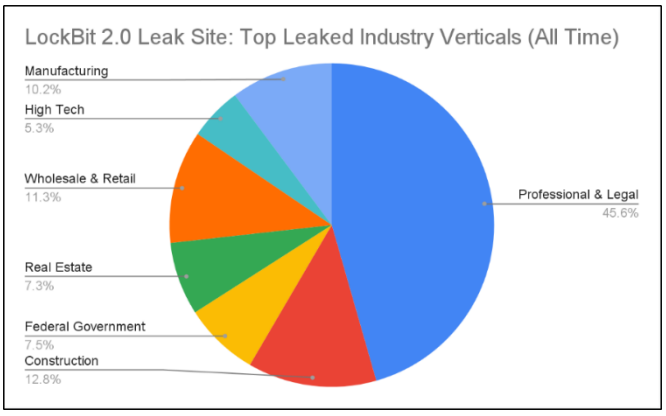


Fig. 1(b)

Figure 1(b) reveals a troubling trend in the most recent analysis of data breaches across various industry sectors. The professional and legal industry appears to be the most vulnerable, with a staggering 45.6% of all leaks. Other significantly impacted sectors include construction, wholesale and retail, and manufacturing, which account for 12.8%, 11.3%, and 10.2% of leaks, respectively. The Federal Government, Real Estate, and High Tech sectors also face considerable threats, contributing to 7.5%, 7.3%, and 5.3% of the total leaks,

respectively. This data underscores the urgent need for robust cybersecurity measures across all sectors, particularly those most at risk.

LockBit's success can be attributed to its strategic recruitment of affiliates and establishment of partnerships with other criminal organizations. The organization employs network access brokers, collaborates with entities such as Maze, and actively seeks out insiders from specific companies. In order to appeal to skilled hackers, they have provided financial support for clandestine technical writing competitions.

LockBit has specifically targeted multiple industries on a global scale, with the healthcare and education sectors being the primary targets. The United States, India, and Brazil are the primary countries targeted in terms of attack attempts. LockBit is highly efficient and versatile malware that strategically highlights its rapidity and advanced features to lure potential victims. When selecting potential victims, they consider external factors such as data privacy laws. LockBit's success also relies heavily on their affiliate program, which helps them innovate and compete in the ransomware landscape.

LockBit introduced an upgraded version of its ransomware in mid-2022, which included a bug bounty program, the use of Zcash for transactions, and novel coercion tactics. This latest iteration integrates components from prominent ransomware strains like BlackMatter and DarkSide. It includes sophisticated techniques to evade detection, executes without relying on passwords, and incorporates a built-in command-line argument function.

The revised ransomware was utilized in cyber assaults targeting the Italian Revenue Agency and a municipal office in Ontario, Canada. LockBit has recently integrated Denial-of-Service attacks into its repertoire, employing them as a supplementary means of exerting pressure in conjunction with encryption and data leaks.

III. METHODOLOGY

2.1 Lockbit 3.0 Encryption Techniques:

The LockBit 3.0 ransomware utilizes a blend of RSA-2048 and AES-256 encryption algorithms to make the files of its victims inaccessible. The ransomware creates an individual RSA-2048 public key for every target, which is utilized to encrypt a randomly generated AES-256 session key for each file. This guarantees that the files can only be decrypted using the corresponding private key possessed by the attacker..

LockBit 3.0 maintains the majority of features found in its previous version, LockBit 2.0, while also incorporating novel behaviors that make it more challenging for researchers to analyze. It operates with LocalServiceNetworkRestricted privileges, obviating the necessity for complete administrator-level authorization. Additionally, it utilizes anti-debugging techniques akin to those employed by BlackMatter, employing ROT13-based hash tables to load/resolve Windows DLLs and obscure internal function calls.

In addition, LockBit 3.0 generates a distinct stub for each API it necessitates, utilizing five distinct types of stubs that can be randomly generated. Every stub is a fragment of shellcode that dynamically performs API hash resolution and directly jumps to the API address stored in memory, thereby increasing the difficulty of reverse-engineering. This summary offers a comprehensive examination of the encryption methods and techniques employed by the LockBit 3.0 ransomware.

2.2 Lockbit 3.0 TTPs

The operational method of a LockBit ransomware operator is defined by a series of complex and detailed procedures. The method begins by examining the external domain space and IP block of the

target organization, usually with the use of scanning tools. The operator thereafter utilizes credentials obtained from other sources to exploit discovered flaws and acquire access.

Upon gaining access, the operator exploits existing vulnerabilities to elevate their privileges. An extensive gathering of data on the affected system follows. Afterwards, the operator guarantees their continued existence in the system and establishes contact with the command and control (C2) infrastructure.

The final phase involves the launch of the ransomware, following which the operator expects communication from the victim. It is essential to comprehend that although certain tools are often associated with these strategies, the actual methods employed might vary and are always developing to evade discovery and countermeasures.

2.3 Infrastructure

Ransomware groups utilize a diverse range of tools and strategies to execute their malevolent activities. They frequently utilize Virtual Private Servers (VPS) from bulletproof hosting providers and data centers, commonly situated in Russia, owing to their unresponsiveness to abuse notifications. Scanners such as Masscan, Nmap, and RustScan are employed to conduct scans on the victim's network's externally facing domain space and IP block. These scans aim to identify accessible services like RDP. They obtain entry into the victim's network by assuming the identity of a valid user through the use of compromised login information. This information is either acquired through purchase from illicit online platforms or by exploiting vulnerabilities in LLMNR and NBT-NS protocols to intercept the administrator's encrypted password. Cloud services, such as private ones accessible on the dark web, Google Colab, and Colabcat, are employed for the purposes of decrypting password hashes or securely storing stolen data. In order to prevent any data from being stored in the file system and to avoid detection by antivirus software, obfuscated stagers employ tools such as Artifact Kit or Shelter Pro. Pentesting tools such as Cobalt Strike, Mimikatz, PowerShell, winPEAS, and linPEAS are employed to establish a connection with the C2 infrastructure, elevate privileges, deactivate security measures, and gather data about the network and the targeted system. Automated frameworks, like BloodHound, are utilized to systematically chart the network and ascertain the most valuable targets. Ultimately, ransomware like LockBit is employed to cipher the files of the target and extort payment.

IV. CASE STUDIES

- CVE-2018-13379: This vulnerability pertains to a path traversal problem found in Fortinet FortiOS and FortiProxy when used in conjunction with the SSL VPN web portal. It allows an unauthenticated attacker to download system files via specially crafted HTTP resource requests.
- CVE-2021-20028: This vulnerability refers to a SQL Injection vulnerability that affects end-of-life Secure Remote Access (SRA) products, specifically the SRA appliances. It occurs due to improper neutralization of a SQL Command.
- CVE-2021-31207: This vulnerability is present in Microsoft Exchange Server and enables an attacker to circumvent the authentication mechanism.
- CVE-2021-34523: The identified vulnerability pertains to an elevation of privilege problem specifically affecting Microsoft Exchange Server.
- CVE-2022-22279: This vulnerability is a post-authentication arbitrary file read vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products.
- CVE-2023-02269: This vulnerability enables remote attackers to circumvent authentication on impacted installations of PaperCut NG.

- CVE-2023-27351: This vulnerability allows unauthorized attackers to potentially access user account information, such as usernames, full names, email addresses, office and department details, and payment card numbers, that are stored in a customer's PaperCut MF and NG servers.

- The vulnerability identified as CVE-2020-0787 affects the Windows Background Intelligent Transfer Service (BITS) and enables an attacker to overwrite a specific file, resulting in an elevated privilege level.

- The vulnerability identified as CVE-2021-22986 exists within the iControl REST API feature of F5's BIG-IP product. An unauthorized, remote attacker can exploit this vulnerability to circumvent authentication and execute unrestricted commands with root privileges.

- CVE-2021-34473: This vulnerability is present in the Autodiscover service of Microsoft Exchange Server and occurs because the URI is not adequately validated before accessing resources.

V. LOCKBIT IMPLEMENTATION AND REVIEW

LockBit 3.0 initiates its attack phase by conducting a debugger evaluation. The program scans for active debuggers and, when found, enters an infinite loop to prevent inspection. Afterwards, the malware performs language checks by utilizing the GetSystemDefaultUILanguage and GetUserDefaultUILanguage methods. Curiously, it excludes Russia and the countries nearby from its roster of affected parties, depending on the language settings.

The next stage entails a deliberate interruption of procedures and amenities. LockBit 3.0 intentionally disables crucial features and terminates processes linked to malware analysis and other applications to evade detection. At the same time, it aims to gain elevated privileges by creating a completely new process and duplicating the token. Upon successful completion, it initiates the execution within DLLHost.exe and terminates the original process.

LockBit 3.0 employs a method that circumvents User Account Control (UAC) to enhance its effectiveness with users. To achieve this, one can inject code into the dllhost.exe process by utilizing the Class Identifiers (CLSIDs) that are linked to COM objects. The malware then duplicates itself within the SYSVOL directory and produces a Group Policy, resulting in the generation of the required XML files.

LockBit 3.0 additionally modifies the configuration of the device. It renders the Windows Defender application inoperative, disabling all notifications, halting the file submission process, and deactivating the real-time protection feature. To spread across the network, the ransomware conducts a thorough scan of all machines in the Active Directory and enforces the recently implemented Group Policy.

LockBit 3.0 employs the "FwPolicy2" object of Windows Defender Firewall to gain entry to and modify firewall rules as a component of its security protocols. Furthermore, it carries out commands to remove shadow copies and actively attempts to disable the recovery function. Furthermore, it eliminates Windows event logs with the intention of concealing its activities.

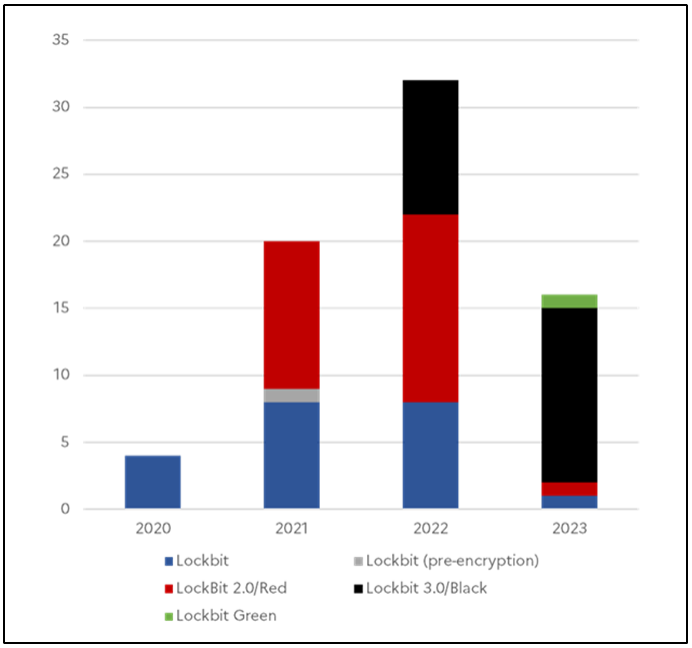
The final phase involves encrypting the system. LockBit 3.0 utilizes encryption to safeguard files and appends the ".HLjkNskOq" file extension to them. The assault sequence reaches its climax with the execution of a ransom letter, which is generated and carried out through the lockbit.hta file. The provided attack sequence demonstrates the sophisticated characteristics and potential damage inflicted by LockBit 3.0 ransomware.

Fig: 1 List of anomalies

VI. IMPACTS AND CHALLENGES

The LockBit ransomware gang showed significant activity between 2020 and 2023, launching a succession of massive operations worldwide. In June 2023, they allegedly penetrated the security of the Taiwan Semiconductor Manufacturing Company (TSMC), claiming a demand for a ransom of $70 million. However, TSMC refuted these allegations. In May 2023, the network of Managed Care of North America (MCNA) Dental was breached, resulting in the compromise of the data of around 9 million patients. In the subsequent month, an Australian engineering business was targeted by a criminal group, which exploited a weakness in the virtual private network (VPN) to obtain unauthorized access. In February 2023, New Zealand saw its inaugural ransomware assault, which specifically targeted a

manufacturing business. In January 2023, Brookfield Residential, a Canadian real estate firm, had a LockBit cyberattack, which led to the encryption of their systems and a subsequent demand for ransom.



In December 2022, the computer system of Regis Healthcare, an elderly care provider in Australia, was infiltrated, resulting in the theft of data prior to the deployment of ransomware. Alico, an agricultural corporation based in Florida, made a payment of $6 million as a ransom in November 2022 due to the encryption of its computers and data. From 2020 to 2022, LockBit carried out several assaults worldwide, specifically targeting vital industries such as governments, hospitals, and infrastructure companies. As a result, LockBit has established itself as one of the most prolific ransomware gangs.

Bl00dy Ransomware Challenge:

The LockBit ransomware gang has had a substantial influence on the field of cybersecurity. The Bl00Dy Ransomware Gang, a recently emerged group, has started employing a leaked LockBit ransomware builder to initiate targeted assaults on corporate entities. The LockBit 3.0 ransomware builder was publicly disclosed on Twitter after a dispute arose between the LockBit operator and their developer. This tool allows individuals to create a functional encryption and decryption device specifically designed for malicious purposes. Anticipating the availability of a customizable configuration file in the builder, it was foreseen that additional malicious actors would promptly exploit the builder to create their own ransomware. This situation highlights the difficulties presented by the LockBit ransomware gang and the possible dangers that exist in the cybersecurity field.

The Bl00Dy Ransomware Gang, which has been active since May 2022, has been specifically targeting different industries, such as medical and dental practices, located in New York. Contrary to conventional ransomware practices that employ Tor data leak websites for blackmail and data disclosure, this criminal group utilizes a Telegram channel. Curiously, the gang does not create its own ransomware but instead utilizes leaked builders and source codes from other operations such as Babuk and Conti.

A new encryptor belonging to the Bl00Dy Ransomware Gang was recently discovered during an attack on a victim in Ukraine. The origin of the ransomware, whether it was derived from Conti or LockBit, was initially ambiguous. However, further verification indicated that the encryptor was constructed using the newly launched LockBit 3.0 builder, as demonstrated by substantial code similarity between Bl00dy and LockBit 3.0 encryptors.

BleepingComputer's testing uncovered notable distinctions between this novel encryptor and its predecessors. Previous campaigns appended the.bl00dy extension to encrypted files. However, due to the absence of a customizable feature in the LockBit 3.0 builder, predetermined extensions were employed instead. However, the file names of the ransom notes still followed the LockBit style,

although they contained personalized text and contact details.
The LockBit operation, initiated in September 2019, has transformed into one of the most dynamic Ransomware-as-a-Service operations. In June 2022, LockBit 3.0 was launched, incorporating novel methods of extortion, a revamped encryptor based on BlackMatter code, and the introduction of the initial ransomware bug bounty program. Given the ease of customization of the leaked LockBit 3.0 ransomware builder, it is anticipated that other threat actors will soon adopt it for their attacks.

ICBC Case:
The Industrial and Commercial Bank of China (ICBC), the country's largest lender, reportedly paid a ransom following a cyberattack by the LockBit ransomware gang. The attack disrupted trades in the U.S. Treasury market and caused a temporary blackout at ICBC's U.S. broker-dealer, leaving it owing BNY Mellon $9 billion. The hack was so extensive that corporate email ceased to function, forcing employees to switch to Google Mail.
The incident occurred amid increased concerns over the endurance of the $26 trillion Treasury market and is going to come under regulatory scrutiny. The Financial Services Information Sharing and Analysis Center highlighted the need for maintaining compliance with every safety precaution and immediately addressing important vulnerabilities, with a specific emphasis on ransomware as a major threat to the financial sector.
LockBit has emerged as a prominent ransomware menace on a worldwide scale, infiltrating major international institutions and exposing confidential information in cases where victims refuse to pay the proposed ransoms. Although authorities encourage the practice, several firms are choosing to pay ransoms in order to immediately recover their systems and prevent damage to their reputations caused by the public disclosure of their data.
Companies' responses to ransomware attacks differ, but a rising variety are compelled to make difficult decisions. Allegedly, the individuals who fell victim to ransomware attacks in 2022 incurred a financial loss of at least $457 million as a result of the actions of the perpetrators. While some firms have successfully recovered their data through the use of backups, this process can be lengthy and does not ensure the desired outcome.
An alternative to ransom payment is to allocate substantial resources towards fortifying defenses to achieve a state of being impervious to hacking, although this approach entails substantial expenses and offers no assurances. If the U.S. government intends to implement a prohibition on ransom payments, it should contemplate providing financial aid to companies to cover the expenses resulting from ransomware attacks. Considering the present condition of U.S. government finances, it appears improbable. Therefore, companies should be ready to shoulder these expenses independently.

VII. PRECAUTIONS AND MITIGATIONS

It is recommended that businesses use particular strategies to lessen the impact on LockBit's operations. The suggested courses of action are in line with the Cross-Sector Cybersecurity Performance Goals (CPGs), which the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA) developed. The CPGs offer a vital set of procedures and safeguards that all organizations should implement, with an emphasis on current cybersecurity frameworks and policies. In order to protect against common and serious cyber threats, these protocols have been developed. Based on the MITRE ATT&CK framework, the mitigations are grouped under the earliest technique that happens in the incident's lifetime. This allows for the inclusion of mitigations that are relevant to multiple tactics. Initial access mitigations would include account usage policies that deal with initial access, persistence, privilege escalation, and credential access.
Organizations must adopt a comprehensive strategy encompassing proactive protection measures, stringent incident response protocols, and data recovery policies in order to effectively mitigate the risks associated with the LockBit ransomware. It is vital to provide all employees with comprehensive security awareness training in order to effectively mitigate threats such as phishing, malware attachments, and suspicious URLs and to aid in the prevention of cybersecurity breaches. In order to

further safeguard against such vulnerabilities, it is critical to consistently apply the most recent security patches for applications, operating systems, and software. Implementing network segmentation solutions can efficiently impede the horizontal propagation of ransomware across an organization's network. Advanced email security solutions fortify the level of protection against an array of methods by which infections can spread. Enabling multi-factor authentication (MFA) for all administrator and remote access accounts is indispensable for preventing potential compromise of your credentials. Critical data can be protected with exceptional efficacy by air-gapped, immutable backup systems. Ransomware attacks are more resistant to isolated backups, which are physically isolated from the network. In contrast, immutable backups ensure data integrity by imposing time limits on illegal modification or deletion. This ensures a trusted source of unaltered data that can be restored in the event of a security breach.

VIII. REFERENCE

1. Abrams, L. (2022, September 28). Leaked LockBit 3.0 builder used by Bl00dy ransomware gang in attacks. BleepingComputer. https://www.bleepingcomputer.com/news/security/leaked-lockbit-30-builder-used-by-bl00dy-ransomware-gang-in-attacks/
2. #StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability | CISA. (2023, November 21). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a
3. A Look at LockBit 3 Ransomware | Red Piranha. (2023, February 22). A Look at LockBit 3 Ransomware | Red Piranha. https://redpiranha.net/news/look-lockbit-3-ransomware
4. Gallagher, S. (2020, October 21). LockBit uses automated attack tools to identify tasty targets. Sophos News. https://news.sophos.com/en-us/2020/10/21/lockbit-attackers-uses-automated-attack-tools-to-identify-tasty-targets/
5. Rochberger, L., & P. (2023, May 16). Threat Alert: Cortex vs. LockBit 3.0 - Palo Alto Networks Blog. Palo Alto Networks Blog. https://www.paloaltonetworks.com/blog/security-operations/threat-alert-cortex-vs-lockbit-3-0/
6. Interview with a LockBit ransomware operator. (2021, February 2). Interview With a LockBit Ransomware Operator. https://blog.talosintelligence.com/interview-with-lockbit-ransomware/
7. What Is LockBit Ransomware? (n.d.). What Is LockBit Ransomware? https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/lockbit
8. JR Gumarin, Abigail Barr, A. E., Elsad, A., Gumarin, J., & Barr, A. (2022, June 9). LockBit 2.0: How This RaaS Operates and How to Protect Against It. Unit 42. https://unit42.paloaltonetworks.com/lockbit-2-ransomware/
9. F. (2023, July 20). LockBit Ransomware: Inside the World's Most Active Ransomware Group. Flashpoint. https://flashpoint.io/blog/lockbit/
10. LockBit ransomware — What You Need to Know. (2023, April 19). www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/lockbit-ransomware
11. XTI, S. (2023, April 27). Dark Web Profile: LockBit 3.0 Ransomware - SOCRadar. SOCRadar® Cyber Intelligence Inc. https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/
12. Milmo, D. (2023, January 13). What is LockBit ransomware and how does it operate? The Guardian. https://www.theguardian.com/business/2023/jan/13/what-is-lockbit-ransomware-and-how-does-it-operate-malware-royal-mail
13. All About LockBit Ransomware - Securin. (2022, March 23). Securin -. https:///articles/all-about-lockbit-ransomware/
14. What Is LockBit Ransomware? (n.d.). What Is LockBit Ransomware? https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/lockbit
15. Understanding Ransomware Threat Actors: LockBit | CISA. (2023, June 14). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

16. Kobialka, D., Kass, D. H., & Masters, J. (2022, April 4). LockBit Ransomware Attack Costs CRM Services Provider Over $42 Million -. MSSP Alert. https://www.msspalert.com/news/lockbit-ransomware-attack-costs-crm-services-provider-over-42-million

17. Understanding Ransomware Threat Actors: LockBit | CISA. (2023, June 14). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a