**The Evolution of LockBit**

**Ransomware: Tactics, Techniques, and Mitigation Strategies**

**By**

**Sathwik Reddy Malreddy**

**Akshaya Dhumala**

**Abhishek Mogili**

**I. Introduction**

**Ransomware** has become a major security risk for businesses all around the world in the last few years. Ransomware is malicious software that extorts money from victims in exchange for the decryption key, encrypting their files. Such cyberattacks can have serious repercussions, including data loss, monetary losses, and even damage to one's reputation.

LockBit is one particularly well-known ransomware strain that has become extremely well-known recently. The goal of this in-depth research is to examine the tactics, methods, and procedures (TTPs) used by the LockBit ransomware during its entire life cycle. We will also examine the extensive worldwide impact that this variation causes (*Cybersecurity Alert - LockBit (Threat Actor) | FINRA.org*, n.d.).

Our goal in carefully analyzing these elements is to offer insightful information about how LockBit functions, assisting organizations in comprehending and counteracting this increasingly dangerous threat. We aim to provide decision-makers with useful information that can help them create successful defenses against ransomware attacks similar to those carried out by LockBit in the future using a combination of technical analysis and real-world case studies.

**II. Origin and Development of LockBit**

As per the insights provided in the article "LockBit Ransomware — What You Need to Know" from 2021, LockBit ransomware has undergone significant transformations. Its inception can be linked back to a preceding ransomware strain identified as ABCD. Activity associated with ABCD was initially detected in September 2019, and by January 2020, a variant of ransomware dubbed LockBit emerged on cybercrime forums primarily in the Russian language sphere.

Since then, LockBit has undergone numerous revisions and iterations, demonstrating constant innovation and development. Version 2 (LockBit 2.0), also known as LockBit Red, was released in June 2021 and included an integrated information-stealing tool called StealBit that increased its functionality. Later, in October 2021, LockBit Linux-ESXi Locker version 1.0 was released, extending its functionality to support VMware ESXi and Linux systems.

LockBit Black (version 3.0) first appeared in March 2022. It shared characteristics with other ransomware variants, including BlackMatter and Alphv (also known as BlackCat). Notably, version 3.0 was made available to non-LockBit affiliates following the builder's leak in September 2022, which increased the platform's impact and reach.

LockBit Green entered the picture in January 2023, using Conti ransomware's source code. This most recent version showed how various components are continuously incorporated into LockBit's functionality, thereby increasing its overall efficacy. Furthermore, on VirusTotal platforms in April, encryptors linked to the LockBit ransomware that target macOS were observed (*LockBit Ransomware — What You Need to Know*, 2021).

**III. LockBit's Tactics, Techniques, and Procedures (TTPs)**

A widely recognized ransomware group called LockBit uses a framework called Ransomware-as-a-Service, or RaaS, in which several affiliates are hired to use LockBit's infrastructure and tools to launch ransomware attacks. LockBit is notable for having a large network of independent affiliates, which leads to a notable variation in the tactics, techniques, and procedures (TTPs) used in LockBit ransomware attacks (Security, 2023).

The diverse array of TTP variations poses a significant obstacle for establishments aiming to maintain network security and combat the threat of ransomware. Because each affiliate takes a unique approach, it becomes harder for defenders to anticipate attacks and effectively stop them. To make matters more complicated, defense strategies are further complicated by LockBit's dynamic nature and the wide range of techniques that its affiliates employ.

**IV. LockBit's Global Impact**

According to Cybersecurity & Infrastructure Security Agency (CISA) (2023), the LockBit ransomware has affected organizations across multiple nations, resulting in a significant global impact. The following data pertains to the operations of LockBit and its effects on the United States:

The proportion of ransomware cases that LockBit is directly responsible for:

* **Australia:** Of Australia's recorded ransomware incidents between April 1, 2022, and March 31, 2023, LockBit was responsible for 18% of them. Not just LockBit 3.0, but all LockBit ransomware variations are covered by this.
* **Canada:** Of the ransomware incidents reported in Canada in 2022, 22% were attributed to LockBit.
* **New Zealand:** Of all ransomware reports for 2022, CERT NZ received 15 reports of LockBit ransomware, accounting for 23% of the total.
* **United States:** LockBit attacks were identified as the cause of about 16% of ransomware incidents in the United States that were reported to the MS-ISAC in 2022. This covers assaults on a range of organizations, including emergency services, county and local governments, and educational institutions.
* **Number of LockBit ransomware attacks in the US since 2020:** 
  + From the time that LockBit activity was first noticed on January 5, 2020, the FBI has reported on about 1,700 LockBit ransomware attacks in the United States (CISA, 2023).
* **US ransoms paid in total to LockBit:**
  + After LockBit's activity was first noticed in the US in January 2020, it is estimated that about $91 million in ransoms have been paid to it. Many reports show how much LockBit has cost the impacted organizations financially (CISA, 2023).

These figures demonstrate the LockBit ransomware's spread and the harm it causes to businesses around the world. The severity of the threat posed by LockBit is demonstrated by the high percentage of incidents that can be attributed to it and the large number of attacks that occur in the United States. The sizeable ransom payments highlight the ransomware operations' financial incentive and the significance of strong cybersecurity defenses against and mitigation of such attacks. It is recommended that organizations exercise caution and implement recommended mitigations to safeguard their networks and data against ransomware threats such as LockBit (CISA, 2023).

According to the Cybersecurity and Infrastructure Security Agency (CISA) report from 2023, a total of 1,653 alleged victims were identified on LockBit leak sites up to Q1 2023. Following the introduction of LockBit 2.0 and LockBit 3.0, changes have occurred in the configuration of leak sites. Some sources have opted to distinguish between leak sites based on different versions of LockBit, while others have chosen not to make such distinctions. As LockBit has evolved over time, both in terms of its functionality and features, the addresses and layouts of its leak sites have undergone alterations, yet they are all grouped under the collective term of LockBit. The launch of LockBit 2.0 towards the end of Q2 2021 had an immediate impact on the cybercriminal market. This impact was notable as several Ransomware-as-a-Service (RaaS) operations, including DarkSide and Avaddon, ceased operations in May and June 2021. LockBit emerged as a competitor against other RaaS entities like Hive RaaS to occupy the void left by these closures, resulting in a surge of LockBit affiliates. The data depicted in Figure 2 illustrates the alleged number of victims worldwide as reported on LockBit leak sites, beginning in Q3 2020.



**Figure:** Alleged Number of Victims Worldwide on LockBit Leak Sites.

**V. Mitigations and Recommendations**

Organizations must follow the guidelines in the Cybersecurity Advisory (CSA) published by the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and international partners in order to successfully reduce the risks related to LockBit ransomware attacks. The recommendations are intended to improve overall cybersecurity posture and strengthen network defenses. Further strengthening resilience against LockBit ransomware incidents can be achieved by aligning with the Cross-Sector Cybersecurity Performance Goals (CPGs), which were created by CISA and the National Institute of Standards and Technology (NIST) (CISA, 2023).

Every phase of a ransomware attack is covered in detail by the CSA's extensive guidelines. These phases include initial access, execution, privilege escalation, defense evasion, credential access, discovery, lateral movement, command and control, exfiltration, and impact (Flashpoint, 2023). The suggested mitigations for each stage should be carefully reviewed by organizations, and appropriate action should be taken. Several significant mitigating factors consist of:

* Initial Access:
  + Implement robust network segmentation to restrict lateral movement.
  + Employ multi-factor authentication (MFA) to protect against unauthorized access.
  + Regularly apply patches and updates to address known vulnerabilities.
* Execution:
  + Employ application whitelisting to allow only trusted programs to execute.
  + Utilize behavior-based detection and endpoint protection solutions to identify malicious activities.
  + Educate employees about phishing and social engineering techniques to prevent inadvertent execution of malicious files.
* Privilege Escalation:
  + Limit administrative privileges and adhere to the principle of least privilege (PoLP).
  + Utilize strong, unique passwords and consider implementing a password manager.
  + Regularly review and update access controls to ensure authorized individuals possess elevated privileges.
* Defense Evasion:
  + Deploy advanced anti-malware solutions integrated with real-time threat intelligence.
  + Implement network and endpoint monitoring to detect and respond to suspicious activities.
  + Regularly backup critical data and store backups offline or in a secure separate environment.
* Credential Access:
  + Enforce strong password policies, including complexity and expiration requirements.
  + Implement multi-factor authentication (MFA) for all accounts, particularly privileged ones.
  + Regularly review and revoke unnecessary or unused credentials.
* Discovery and Lateral Movement:
  + Monitor network traffic for abnormal or suspicious patterns.
  + Implement network segmentation to limit the potential impact of lateral movement.
  + Regularly conduct vulnerability assessments and penetration testing to identify and remediate vulnerabilities.

Importantly, these mitigations ought to be put into practice as a component of a thorough defense-in-depth plan. Establishing best practices, conducting risk assessments, and verifying security controls on a regular basis are all important for organizations. Continual staff education and awareness campaigns can also aid in averting successful ransomware attacks by encouraging an organization-wide security-conscious mindset (CISA, 2023).

**VI. Conclusion**

The LockBit ransomware has become a significant global threat, impacting businesses in a variety of industries. To create strong defenses and mitigations against this threat, it is essential to have a thorough understanding of LockBit's history and current state. Using a Ransomware-as-a-Service (RaaS) business model, LockBit relies on affiliates who use its infrastructure and tools to launch attacks. The large number of unconnected affiliates leads to differences in tactics, procedures, and techniques (TTPs), which is a problem for organizations trying to protect themselves from LockBit attacks.

Organizations must constantly modify and improve their cybersecurity protocols due to the dynamic nature of ransomware threats. Maintaining an advantage over threat actors requires proactive deployment of strong security controls and adherence to best practices. In order to share information, exchange intelligence, and develop effective countermeasures against ransomware, cooperation between law enforcement agencies, cybersecurity groups, and international partners is essential (*LockBit Ransomware — What You Need to Know*, 2021).

It is impossible to overestimate the necessity of ongoing cybersecurity measure improvement. Effective ransomware threat mitigation requires regular security posture assessments, thorough risk assessments, and strategic investments in technologies and procedures. Resilience against LockBit ransomware and other emerging threats can be greatly increased by putting the suggested mitigations into practice, aligning with performance goals that have been set, such as those established by industry standards, and cultivating a culture of cybersecurity awareness throughout the entire organization.

**References**

* CISA. (2023, June 14). *Understanding Ransomware Threat Actors: LockBit | CISA*. Www.cisa.gov. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
* *Cybersecurity Alert - LockBit (Threat Actor) | FINRA.org*. (n.d.). Www.finra.org. Retrieved February 28, 2024, from https://www.finra.org/rules-guidance/guidance/cybersecurity-alert-lockbit-threat-actor-012524
* Flashpoint. (2023, July 20). *LockBit Ransomware: Inside the World’s Most Active Ransomware Group*. Flashpoint. https://flashpoint.io/blog/lockbit/
* *LockBit ransomware — What You Need to Know*. (2021, January 13). Usa.kaspersky.com. https://usa.kaspersky.com/resource-center/threats/lockbit-ransomware
* Security, C. C. for C. (2023, June 14). *Understanding ransomware threat actors: LockBit - joint cybersecurity advisory*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/understanding-ransomware-threat-actors-lockbit-joint-cybersecurity-advisory