LockBit Ransomware – OSINT Threat Intelligence Report

Prepared by: Srishti Rathi
Date: 2025
Type: OSINT-based Threat Intelligence Analysis

Executive Summary

LockBit is a prominent ransomware threat operating under a **Ransomware-as-a-Service (Raas)** model, responsible for a significant number of global ransomware incidents between **2021 and 2023**. The group enables affiliates to deploy ransomware in exchange for a share of ransom payments, allowing paid scalability and widespread operational reach. LockBit was identified as **the most prolific ransomware group in 2022,** impacting organizations across multiple industries worldwide.

OSINT analysis indicates that LockBit activity has been predominantly observed in countries such as the **United States, India, and Brazil,** with frequent **targeting of healthcare and educational institutions** due to their critical services, limited downtime tolerance, and constrained incident response capabilities. LockBit is widely known for employing **double extortion tactics,** combining data encryption with threats of public data disclosure to increase coercive pressure on victims.

The group maintains an active affiliate recruitment ecosystem through underground forums, leak sites, and incentive-driven programs, reflecting a mature and highly organized cybercriminal operation. LockBit's evolving tactics, affiliate-driven model, and continued re-emergence following law enforcement disruptions present a persistent and adaptable threat to organizations globally.

Threat Actor Overview

LockBit is a financially motivated cybercriminal group operating under a **Ransomware-as-a-Service (RaaS)** business model. The core LockBit operators are responsible for developing and maintaining the ransomware payload, command-and-control(C2) infrastructure, payment portals, and data leak sites. Independent affiliates carry out intrusions and deploy the ransomware in victim environments, receiving a percentage of ransom payments as compensation.

This decentralized structure enables LockBit to scale rapidly, conduct simultaneous attacks across multiple geographic regions, and adapt tactics based on **affiliate** capabilities. Affiliates range from highly skilled cybercriminals to opportunistic actors leveraging purchased access, phishing campaigns, or exploitation of exposed services.

LockBit primarily targets organizations within **healthcare, education, manufacturing, logistics, and critical infrastructure sectors**, selecting victims with high operational dependency on data availability and an increased likelihood of ransom payment.

Infrastructure & Tooling (OSINT-Based)

OSINT reporting indicates that LockBit operates a distributed infrastructure designed to support affiliate activity and victim interaction. Observed infrastructure components include:

- **Tor-based leak sites** used to public stolen victim data and apply reputational pressure
- **Ransom payment portals** accessible via Tor
- **Affiliate panels** enabling campaign management and payload customization
- **Command-and-Control (C2) servers** for payload execution and telemetry
- **StealBit,** a custom data exfiltration tool introduced in LockBit 2.0

LockBit affiliates commonly leverage publicly available and living-off-the-land tools (LOLBins), including:

- PowerShell
- PsExec
- SMB and Windows Admin Shares
- Credential dumping utilities (e.g., Mimikatz)

This tooling strategy reduces dependency on custom malware and complicates detection by blending malicious activity with legitimate administrative behavior.

MITRE ATT&CK; Mapping

Initial Access

- Phishing – **T1566**
- Exploitation of Public-Facing Applications – **T1190**
- Abuse of Valid Accounts – **T1078**
- External Remote Services – **T1133**

Execution & Persistence

- PowerShell – **T1059.001**
- Command-Line Interface – **T1059**
- Scheduled Tasks – **T1053**

Credential Access

- Credential Dumping – **T1003**

Lateral Movement

- SMB/Windows Admin Shares – **T1021.002**

Exfiltration

- Exfiltration to Cloud Storage – **T1567.002**
- Exfiltration Over Web Services – **T1567**

Impact

- Data Encrypted for Impact – **T1486**
- Defacement (Wallpaer Modification) – **T1491.001**

Indicators of Compromise (IOCs)

Behavioral Indicators

- Creation of ransom note files (e.g., <Ransomware_ID>.README.txt)
- Sudden mass file encryption across endpoints and network shares
- Wallpaper or desktop background changes displaying LockBit branding
- High-volume SMB traffic between internal hosts
- Unauthorized execution of PowerShell and PsExec commands

Network Indicators

- Outbound connections to Tor nodes
- Unusual connections to cloud-based file hosting services (e.g., MEGA, rclone endpoints)
- Communication with previously unseen external IP addresses during late-night hours

Risk Assessment

Threat Level: High

LockBit poses a high risk to organizations due to:

- Its mature RaaS ecosystem
- Aggressive affiliate recruitment
- Effective double extortion tactics
- Broad targeting across industries
- Continued operational resilience following law enforcement disruption

Organizations with exposed remote access services, weak credential hygiene, limited segmentation, or insufficient monitoring are at elevated risk of compromise.

Mitigation Recommendations

To reduce exposure to LockBit ransomware activity, organizations should implement the following controls:

1. Deploy multi-layered security defenses across endpoints, networks, and email gateways
2. Enforce network segmentation to limit lateral movement
3. Implement multi-factor authentication (MFA) for RDP, VPN, and privileged accounts
4. Maintain offline and immutable backups with regular restoration testing
5. Conduct continuous allow-listing, patch management, and vulnerability scanning
6. Enable centralized logging and SIEM-based monitoring
7. Restrict PowerShell execution and administrative tool usage through policy controls
8. Monitor for abnormal file encryption behavior and mass SMB activity

Methodology & Disclaimer

This report is based solely on open-source intelligence collected from public advisories, technical reports, and threat research. Findings are intended for educational and defensive security purposes only.