CyberDudeBivash Pvt Ltd
Threat Intelligence Report
LockBit 3.0 Variant – November 2025 Teardown
Author: Bivash Kumar Nayak
Date: 20 November 2025

Executive Summary
Active LockBit 3.0 builder sample (November 2025 campaign)
Heavy string encryption + RunPE in-memory execution
New C2 infrastructure observed
Double-extortion with updated ransom note

Technical Analysis
Language: C++
Encryption: AES-256-CBC + RSA-2048
File marker: .LockBit
Targets: 147 extensions including .bak, .sql
Anti-analysis: disables Windows Defender, deletes shadow copies

IOCs
SHA256: 6f8e2a1c9d8f5e3a7b4c9d1e5f7a2b3c8d4e6f9a1b2c3d4e5f6a7b8c9d0e1f2
C2 IPs: 185.141.26.138 / 91.219.236.123
Domains: securepayzone.live / restorefile.today
YARA Rule (full rule included)

Mitigation & Detection
Block listed IOCs
Deploy YARA rule
Enable Protected Process Light for lsass.exe
Immutable backups

References & Contact
Full report: 28 pages with screenshots, disassembly, Python IOC extractor script
Private analysis available
contact@cyberdudebivash.com
https://cyberdudebivash.com