LockBit 3.0 Leaks 600 GBs of Data Stolen From Indian Lender

By Jayant Chakravarti

Archived: 2026-04-05 17:45:06 UTC

Fraud Management & Cybercrime , Geo Focus: Asia , Geo-Specific

Data Leak Comes After Fullerton India Refused to Negotiate With Ransomware Group (@JayJay_Tech) • May 8, 2023

The LockBit 3.0 ransomware group on Monday leaked 600 gigabytes of critical data stolen from Indian lender Fullerton India, two weeks after the group demanded a $3 million ransom from the company.

See Also: Experts Offer Insights from Theoretical to the Realities of AI-enabled Cybercrime

Fullerton India said on April 24 that it had suffered a malware attack that forced it to temporarily operate offline as a precaution. The company said it had resumed customer services and worked with global cybersecurity experts to make its security environment more resilient.

The ransomware group soon listed Fullerton India as a victim on its data leak site, stating it had stolen more than 600 gigabytes of "loan agreements with individuals and legal companies."

The group set a deadline of April 29 for the company to pay the ransom to keep the group from publishing the stolen data. The group also gave the company the option to pay $1,000 to extend the deadline by 24 hours.

Fullerton India operates 699 branches across India that offer doorstep credit services to around 2.1 million customers. The company in 2022 had more than $2.5 billion worth of assets under management and employed

over 13,000 people.

Ritesh Bhatia, noted cybercrime researcher and the founder of V4WEB Cybersecurity, shared evidence with Information Security Media Group about the LockBit group releasing documents related to Fullerton India on the dark web. He said the data leak occurred as a result of Fullerton India refusing to engage with the ransomware group, leading to the group initiating triple-extortion tactics to force the company to pay.

While double extortion involves ransomware actors encrypting a victim's data and exfiltrating it to place additional pressure on the victim to pay, a triple-extortion tactic involves hackers contacting the victim's clients, business partners, vendors and customers to make the breach public and force the victim to come to the negotiating table.
