LockBit ransomware gang claims PayBito crypto exchange as new victim

By Waqas

Published: 2022-02-05 · Archived: 2026-04-05 20:39:57 UTC

LockBit ransomware operators claim that they stole the PayBito database that contains 100,000 customers' information including email addresses and "weak" password hashes.

The infamous **LockBit ransomware gang** is claiming to have hacked PayBito, a global cryptocurrency exchange, and stolen its data including a database with 100,000 customers' information.

The group claimed the attack on Thursday, February 3rd on its official website on the so-called **dark web accessible through the Tor browser**. In its post, the operators of LockBit ransomware stated the stolen database contains personal information of customers in the United States and other countries worldwide.

It further claimed that the stolen records have email addresses and a "weak hash algorithm" referring to a password algorithm that can be easily decrypted into cleartext format. Additionally, the alleged data includes the personal data of the exchange's administrators.

> *"Crypto exchange of "HashCashConsultant" company, > 100k Users in DB. Customers from USA/WorldWide personal data, mail/hash, weak hash algorithm. Admins personal data, admin emails, and hashes. If you want to buy it – contact us with TOX – All available data will be published."*
>
> *LockBit*

It is worth noting that the PayBito exchange offers buying, selling, and trading of Bitcoin, Ether, Bitcoin Cash, Litecoin, and several other cryptocurrencies. The exchange is managed by **HashCash**, a Palo Alto, California-based global blockchain and IT services company.

Post published by LockBit ransomware gang on its official website (Image credit: Hackread.com)

Threat intelligence feeds like Dark Tracer and Dark Feed have also tweeted (**1** & **2**) about the alleged ransomware attack on PayBito. Nevertheless, the bad news is that LockBit plans to publish the alleged stolen records on February 21st, 2022 if their demand for ransom is not met.

History of LockBit ransomware gang

Like other ransomware gangs, LockBit's modus operandi involves blocking victims' access to computer systems in exchange for a ransom payment. LockBit, which itself is a malicious software, automatically vets for valuable targets, spreads the infection, and encrypts all accessible computer systems on a network.

The Lockbit ransomware gang emerged on the threat spectrum back in September 2019 and made waves in June 2021 after launching LockBit 2.0 and recruiting new partners. The gang claims to offer the "fastest data exfiltration on the market through StealBit," noted Emsisoft in the gang's **profile**.

StealBit is a data stealer that can download 100 GB of data from an infected system within 20 minutes. Some of the gang's previous victims include **Bangkok Airways**, **Accenture**, **Businesses in Europe**, and **French Ministry of Justice**, etc.

As for the alleged ransomware attack on PayBito, at the time of publishing this article, the exchange or HashCash had not released any statement to address the issue. However, Hackread.com has contacted the company and this article will be updated based on their confirmation or denial.

More ransomware news on Hackread.com

Ransomware attack on New Mexico jail put prisoners in lockdown

Europol takes down VPN service VPNLab used by ransomware operators

FBI warns of hackers mailing malicious USB drives to spread ransomware

Microsoft: 'Destructive malware' fakes ransomware to target Ukrainian orgs

Cyber-Partisans hackers hit Belarus railroad system with a ransomware attack

---