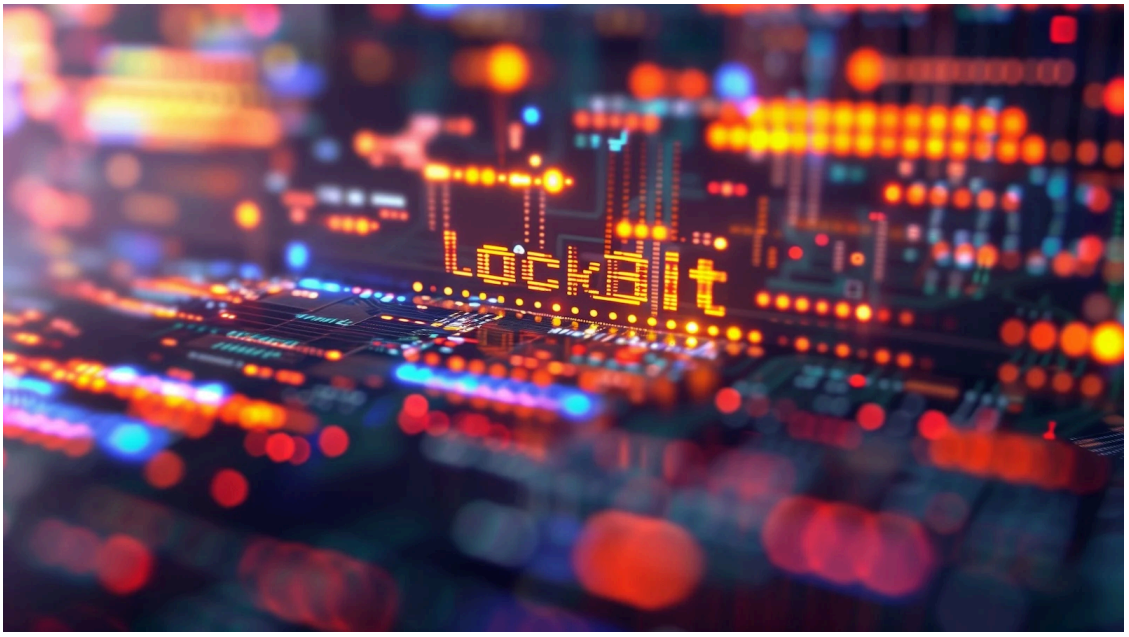
LockBit ransomware gang has over $110 million in unspent bitcoin

By Ionut Ilascu

Published: 2024-02-23 · Archived: 2026-04-05 15:30:52 UTC

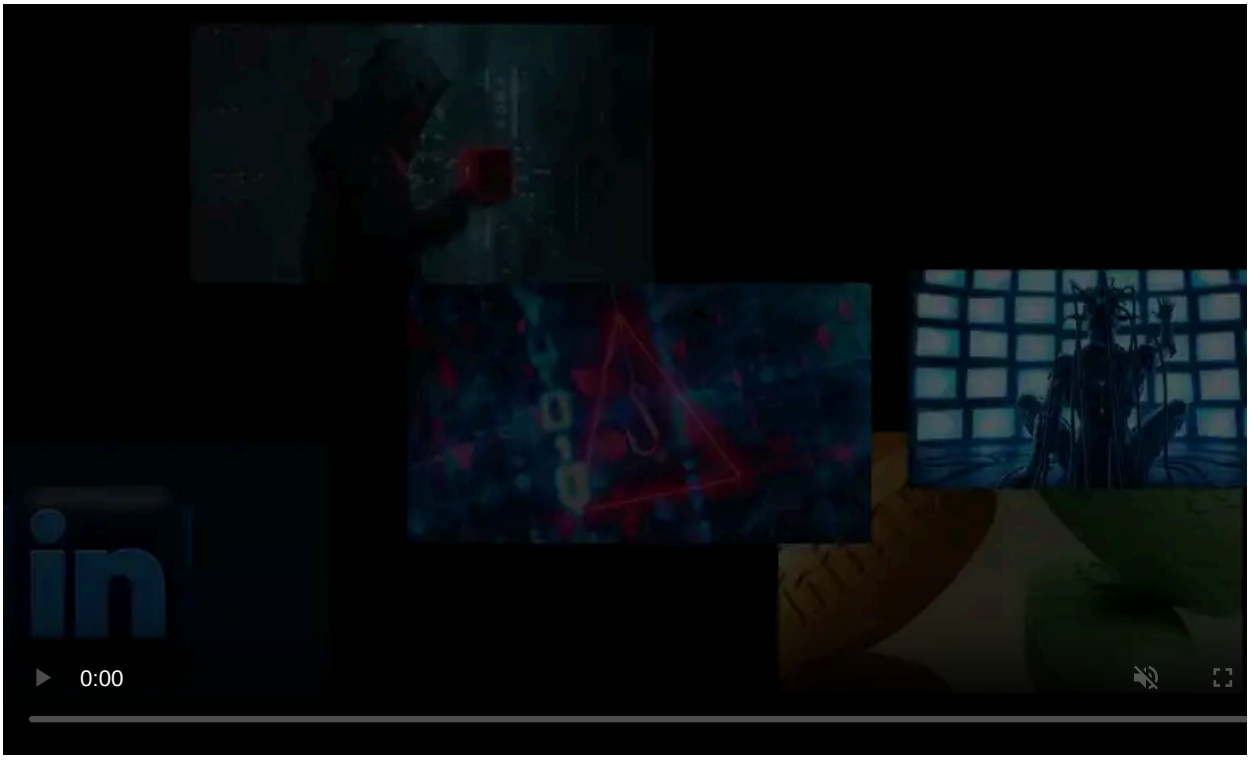


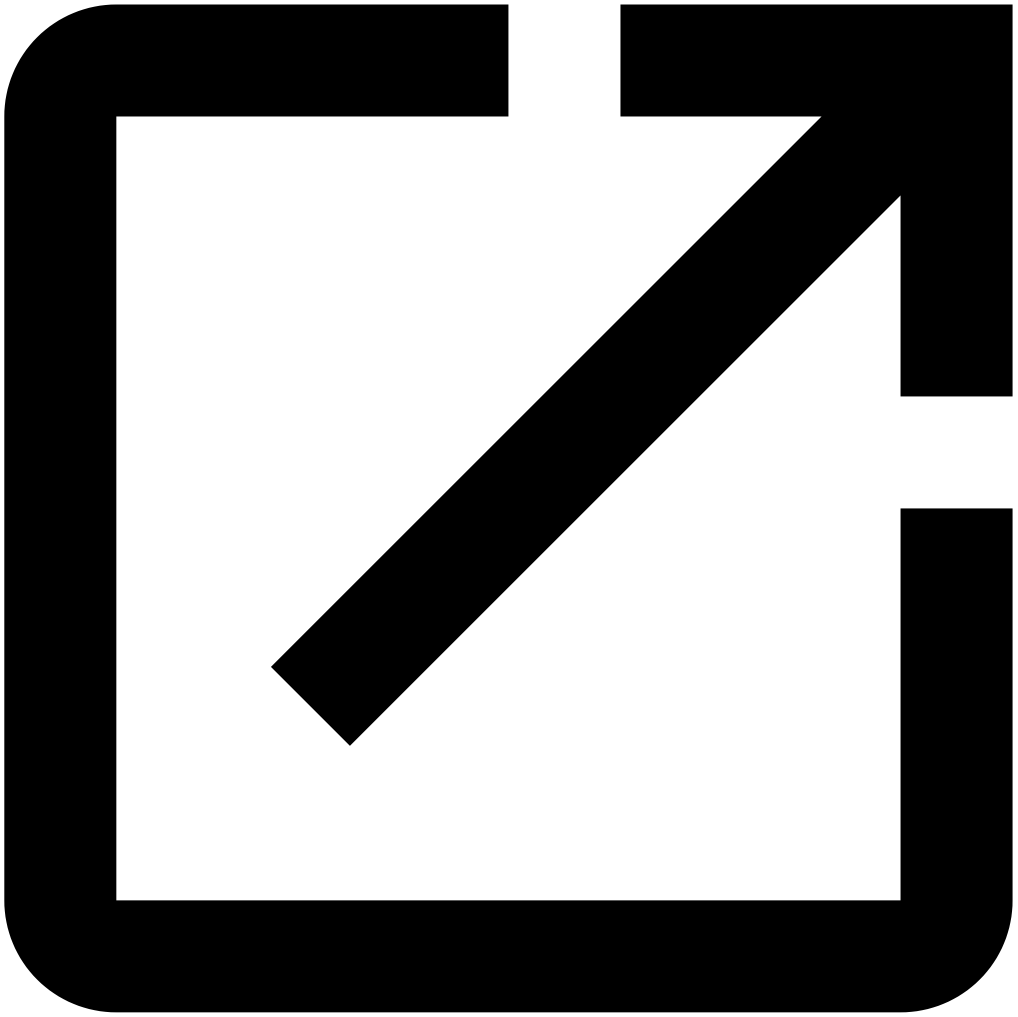
The LockBit ransomware gang received more than $125 million in ransom payments over the past 18 months, according to the analysis of hundreds of cryptocurrency wallets associated with the operation.

Following the LockBit takedown in Operation Cronos, the National Crime Agency (NCA) in the U.K. with support from blockchain analysis company Chainalysis identified more than 500 cryptocurrency addresses being active.

LockBit's money

After hacking LockBit's infrastructure, law enforcement obtained 30,000 Bitcoin addresses used for managing the group's profits from ransom payments.


0:00



More than 500 of these addresses are active on the blockchain and received over $125 million (at current Bitcoin value) between July 2022 and February 2024.

The investigation found that more than 2,200 BTC - more than $110 million at today's exchange rate, remained unspent when LockBit was disrupted.

A press release from the NCA today notes that "these funds represent a combination of both victim and LockBit payments" and that a significant part of this money represents the 20% fee that affiliates paid to the ransomware developers.

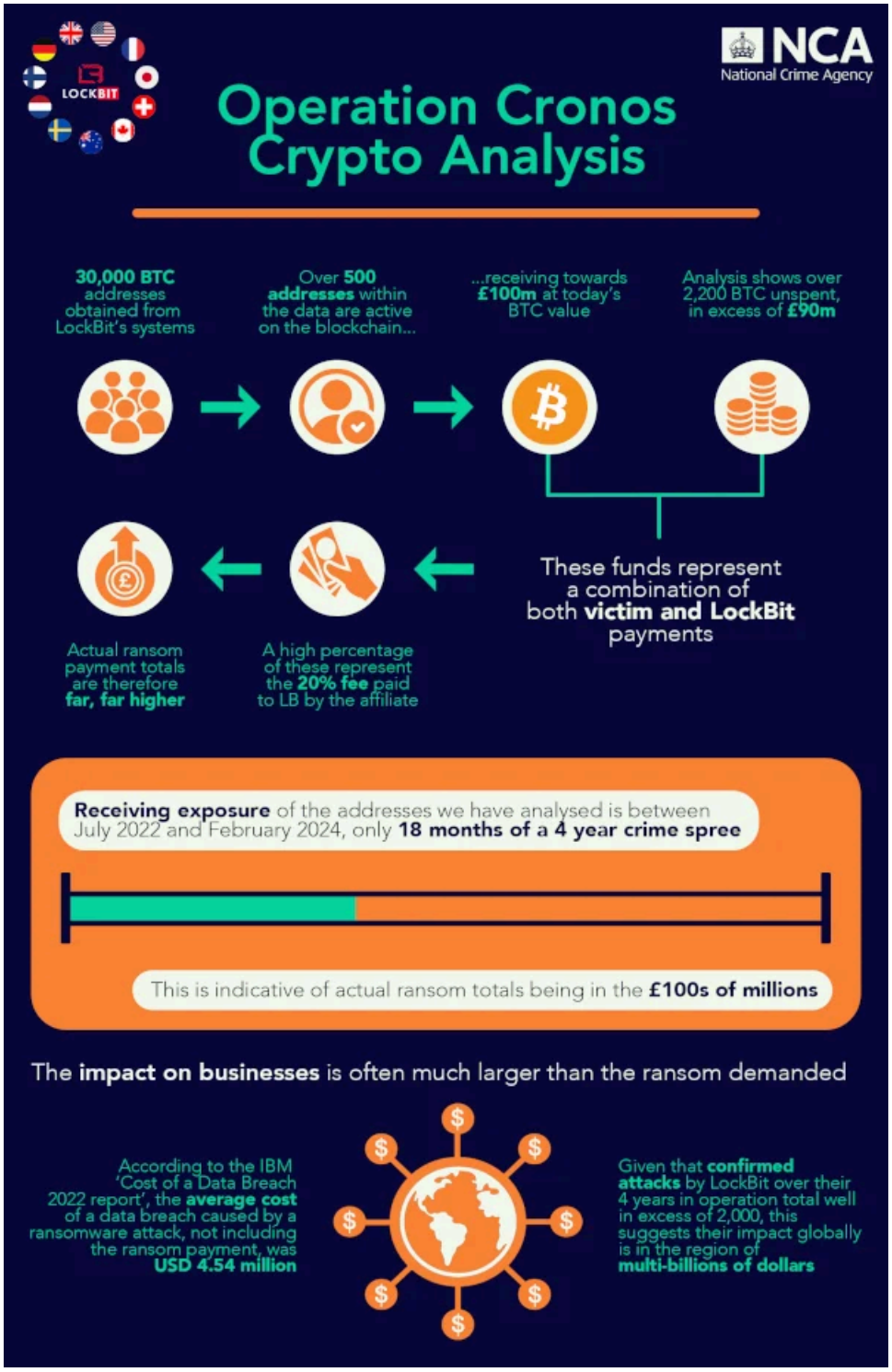
This means that the total figure for the ransoms victims paid to avoid a data leak is "far, far higher," the NCA explains.

(As the agency highlighted, the threat actor did not always delete stolen data, or all of it, even if the victim paid the ransom)

The law enforcement agency says that the amounts discovered in the investigation indicate that the actual ransom totals are in the hundreds of millions.

It is worth highlighting that the impressive amounts are representative only of 18 months of LockBit's cybercriminal activity.

"Given that confirmed attacks by LockBit over their 4 years in operation total well over 2,000, this suggests that their impact globally is in the region of multi-billions of dollars" - UK's National Crime Agency



LockBit had $110+ million in 2,200 unspent bitcoins

source: NCA

In mid-June 2023, America's Cyber Defense Agency (CISA) said that LockBit was responsible for 1,700 ransomware attacks in the U.S. since 2020 and the gang extorted victims of $91 million.

The NCA also said that taking over LockBit's infrastructure led to the discovery of 85 cryptocurrency exchange accounts, now restricted by Binance, with hundreds of thousands of USD worth of crypto assets.

Almost four years in the game

LockBit emerged in September 2019 (as ABCD) and focused on high-profile organizations such as Boeing, the UK Royal Mail, Continental, Bangkok Airways, and Accenture.

It became the most active ransomware group, being responsible for most attacks of this type in 2023, switching between multiple file encrypting malware over the years (LockBit 2.0, LockBit 3.0, LockBit Green) and a new one in the works.

At the time of its disruption, the LockBit group was also the oldest on the ransomware scene, and likely one of the largest with close to 200 affiliates.

Law enforcement in 10 countries collaborated to take control of the threat actor's infrastructure, coordinate the disruption, collect information from the servers, make arrests, and impose sanctions.

Although the hackers' infrastructure is controlled by law enforcement, the leaders of the group and most affiliates are yet to be identified.

The U.S. State Department is offering up to $15 million in rewards to anyone who can provide information about LockBit ransomware gang members and their partners.

Source: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-has-over-110-million-in-unspent-bitcoin/