# LockBit lied: Stolen data is from a bank, not US Federal Reserve

By **Ax Sharma**

June 26, 2024 02:20 PM 6


Recently-disrupted LockBit ransomware group, in a desperate attempt to make a comeback, claimed this week that it had hit the Federal Reserve, the central bank of the United States.

The tall claim was followed up with LockBit stating it had stolen 33 terabytes of sensitive banking information belonging to Americans and that negotiations were ongoing.

Except, the rumor has been quashed. Turns out, the threat actor hit an individual bank, and not the Fed.

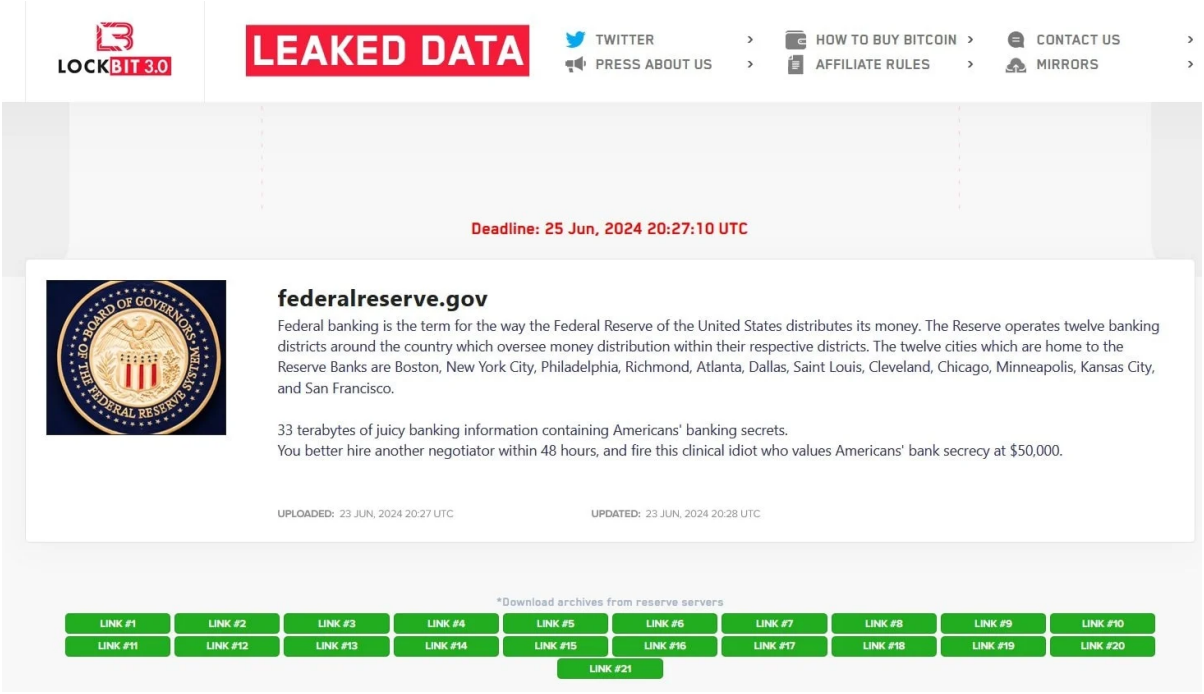
## Bold claims

On Sunday, June 23rd, the LockBit ransomware gang announced that it had breached the Federal Reserve (aka The Fed), the most powerful economic institution in the United States.

"33 terabytes of juicy banking information containing Americans' banking secrets," claimed LockBit on its leak site, alluding to the group having breached the Fed's systems and stolen sensitive data.

The ransomware operator further suggested that negotiations were ongoing and that a "clinical idiot" offered them $50,000 to not leak the data.

"You better hire another negotiator within 48 hours, and fire this clinical idiot who values Americans' bank secrecy at $50,000."




**LockBit claims it attacked the Fed, leaks data** (Hackmanac)

Eventually, the group began publishing the stolen data on its site.

Some media outlets reported on the allegation without obtaining a statement from the Federal Reserve or verifying if the organization was even attacked as LockBit claims.

It turns out that it's not the Fed but an individual US financial institution that the threat actors have targeted in this attack.

"They have apparently breached the American bank Evolve Bank & Trust," cyber threat monitoring company, HackManac posted in an update on social media.

"For now, there is still no trace of 'secret' files, but the analysis is ongoing."

BleepingComputer reached out to Evolve Bank & Trust with questions related to the attack and the financial institution has confirmed that threat actors have "illegally" obtained data from its systems.

"Evolve is currently investigating a cybersecurity incident involving a known cybercriminal organization. It appears these bad actors have released illegally obtained data, on the dark web," an Evolve Spokesperson told BleepingComputer.

"We take this matter extremely seriously and are working tirelessly to address the situation. Evolve has engaged the appropriate law enforcement authorities to aid in our investigation and response efforts. This incident has been contained, and there is no ongoing threat."

"In response to this event, we will offer all impacted customers (end users) complimentary credit monitoring with identity theft protection services. Those affected will be contacted directly with instructions on how to enroll in these protective measures. Additionally, impacted customers will receive new account numbers if warranted."

"Updates and further information will be posted on our website as they become available."

We asked Evolve if it knew exactly when the threat actors had stolen this data, and how the bank's systems were breached.

"No further comments will be made during investigation," Evolve further responded to BleepingComputer.

We also attempted to reach out to LockBitSup, the manager of the ransomware operation, but it appears we have been blocked by him.

Interestingly, recently the Federal Reserve had penalized Evolve Bank & Trust over multiple "deficiencies" identified in how the bank conducted risk management, anti-money laundering (AML), and compliance practices.

Examinations conducted in 2023 found that the bank had "engaged in unsafe and unsound banking practices by failing to have in place an effective risk management framework for those partnerships."

As a result, the Fed demanded that Evolve halt some of its activities until the bank improves its risk management policies and complies with AML laws and regulations.

## "A desperate bid for relevance"

Reacting to the ransomware operator's baseless claims, X account AzAl Security dubbed this as LockBit's "desperate bid for relevance."

> *The Sensationalism of LockBitSupp: A Desperate Bid for Relevance*
>
> *LockBitSupp has resorted back to sensationalism to maintain relevance (remember the Mandiant claim?) This is a clear sign of his continued fall from grace within the Russian ransomware scene. By claiming to have...*
>
> — AzAl Security (@azalsecurity) June 26, 2024

Previously notorious for executing ransomware attacks on high-profile targets like Boeing, the Continental automotive giant, the Italian Internal Revenue Service, Bank of America, the UK Royal Mail, and most recently London Drugs, the cybercrime group found itself in hot waters this year.

In February, law enforcement took down LockBit's infrastructure in an action known as Operation Cronos and seized 34 servers containing over 2,500 decryption keys that helped create a free LockBit 3.0 Black Ransomware decryptor.

Having thrived through its peak, LockBit seems to have entered tough times, compelling it to resort to making misleading claims to stay relevant.

FEDERAL RESERVE BANK | LOCKBIT | LOCKBIT 2.0 | LOCKBIT 3.0

## AX SHARMA

Ax Sharma is an Indian-origin British security researcher and journalist focused on malware analyses and cybercrime investigations. His areas of expertise include open source software security, threat intel analysis, and reverse engineering. Frequently featured by leading media outlets like the BBC, Channel 5, Fortune, WIRED, among others, Ax is an active community member of the OWASP Foundation and the British Association of Journalists (BAJ). Send any tips via email or Twitter DM.

PREVIOUS ARTICLE NEXT ARTICLE

## Comments

**DyingCrow** - 1 day ago

Looks like more about ego then money?

**Hmm888** - 1 day ago

Money is no longer the primary motivation. As a member of this site, you should already be aware of this.

The main goal now is to highlight the gross negligence and complacency in the privacy and security practices of major computer systems. Attackers seldom target Asian systems. Instead, they focus on North America, using it as a "test" market to expose the vulnerabilities and lax security measures of IT administrators and corporations.

As long as ransomware insurance is available and there are no criminal penalties for companies that fail to mitigate risks and disregard privacy, these issues will persist, particularly in North America.

**NoneRain** - 19 hours ago

If you're referring to state sponsored actors, yes, they're not primally moved by financial gains. Otherwise, ransom gangs are. RaaS and MaaS are there, you know.

**shenanigansToo** - 19 hours ago

"The main goal now is to highlight the gross negligence and complacency in the privacy and security practices of major computer systems. Attackers seldom target Asian systems"

I don't believe there is much evidence to support that motivations have changed significantly. Furthermore, Asia is increasingly being targeted. https://www.weforum.org/agenda/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/

**ctigga** - 1 day ago

Money is most definitely the motivation for nearly all of these criminals.
I suspect most also have an ego/think they are pretty smart...until they're busted :D

**Hmm888** - 1 day ago

"Money is most definitely the motivation for nearly all of these criminals.
I suspect most also have an ego/think they are pretty smart...until they're busted :D"

That's now a myth.