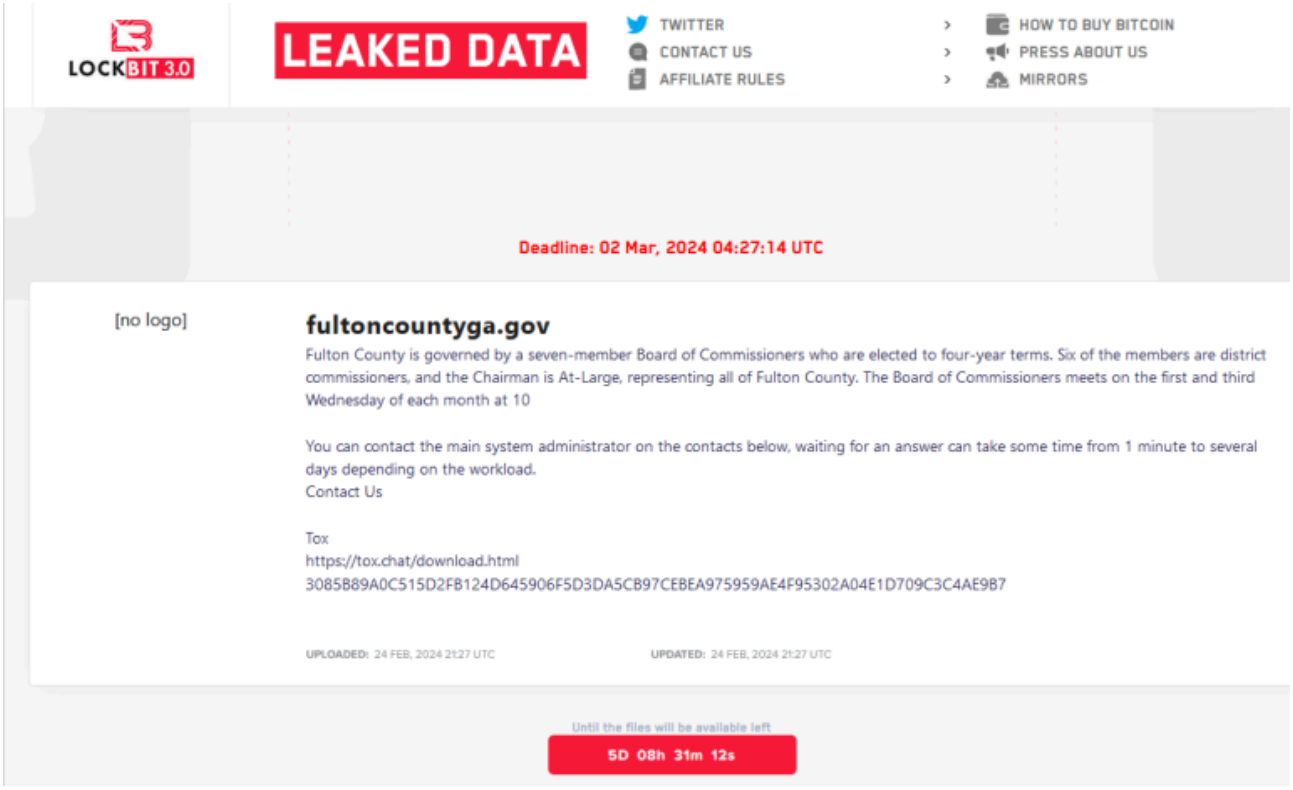
Fulton County, Security Experts Call LockBit's Bluff

Published: 2024-02-29 · Archived: 2026-04-05 18:20:13 UTC

The ransomware group **LockBit** told officials with **Fulton County, Ga.** they could expect to see their internal documents published online this morning unless the county paid a ransom demand. LockBit removed Fulton County's listing from its victim shaming website this morning, claiming the county had paid. But county officials said they did not pay, nor did anyone make payment on their behalf. Security experts say LockBit was likely bluffing and probably lost most of the data when the gang's servers were seized this month by U.S. and U.K. law enforcement.



The LockBit website included a countdown timer until the promised release of data stolen from Fulton County, Ga. LockBit would later move this deadline up to Feb. 29, 2024.

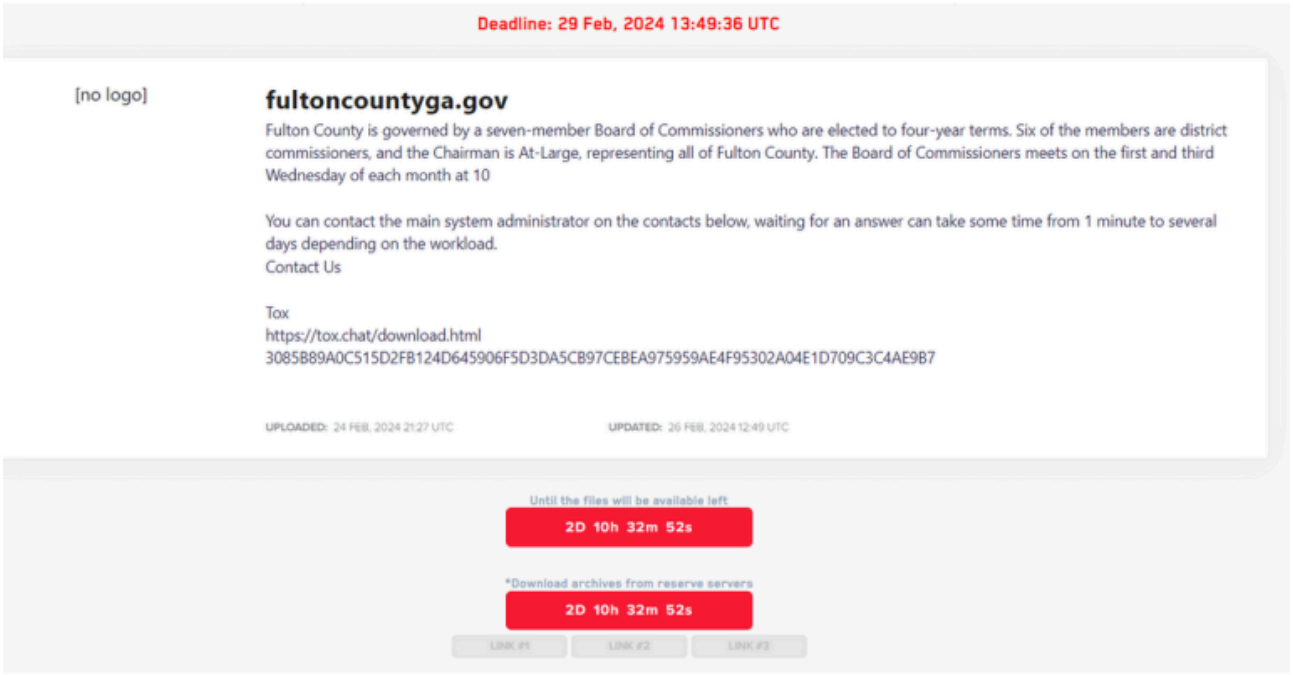
LockBit listed Fulton County as a victim on Feb. 13, saying that unless it was paid a ransom the group would publish files stolen in a breach at the county last month. That attack disrupted county phones, Internet access and even their court system. LockBit leaked a small number of the county's files as a teaser, which appeared to include sensitive and sealed court records in current and past criminal trials.

On Feb. 16, Fulton County's entry — along with a countdown timer until the data would be published — was removed from the LockBit website without explanation. The leader of LockBit told KrebsOnSecurity this was because Fulton County officials had engaged in last-minute negotiations with the group.

But on Feb. 19, investigators with the FBI and the U.K.'s National Crime Agency (NCA) took over LockBit's online infrastructure, replacing the group's homepage with a seizure notice and links to LockBit ransomware decryption tools.

In a press briefing on Feb. 20, **Fulton County Commission Chairman Robb Pitts** told reporters the county did not pay a ransom demand, noting that the board "could not in good conscience use Fulton County taxpayer funds to make a payment."

Three days later, LockBit reemerged with new domains on the dark web, and with Fulton County listed among a half-dozen other victims whose data was about to be leaked if they refused to pay. As it does with all victims, LockBit assigned Fulton County a countdown timer, saying officials had until late in the evening on March 1 until their data was published.



LockBit revised its deadline for Fulton County to Feb. 29.

LockBit soon moved up the deadline to the morning of Feb. 29. As Fulton County's LockBit timer was counting down to zero this morning, its listing disappeared from LockBit's site. LockBit's leader and spokesperson, who goes by the handle "**LockBitSupp**," told KrebsOnSecurity today that Fulton County's data disappeared from their site because county officials paid a ransom.

"Fulton paid," LockBitSupp said. When asked for evidence of payment, LockBitSupp claimed. "The proof is that we deleted their data and did not publish it."

But at a press conference today, Fulton County Chairman Robb Pitts said the county does not know why its data was removed from LockBit's site.

"As I stand here at 4:08 p.m., we are not aware of any data being released today so far," Pitts said. "That does not mean the threat is over. They could release whatever data they have at any time. We have no control over that. We

have not paid any ransom. Nor has any ransom been paid on our behalf."

Brett Callow, a threat analyst with the security firm **Emsisoft**, said LockBit likely lost all of the victim data it stole before the FBI/NCA seizure, and that it has been trying madly since then to save face within the cybercrime community.

"I think it was a case of them trying to convince their affiliates that they were still in good shape," Callow said of LockBit's recent activities. "I strongly suspect this will be the end of the LockBit brand."

Others have come to a similar conclusion. The security firm **RedSense** posted an analysis to Twitter/X that after the takedown, LockBit published several "new" victim profiles for companies that it had listed weeks earlier on its victim shaming site. Those victim firms — a healthcare provider and major securities lending platform — also were unceremoniously removed from LockBit's new shaming website, despite LockBit claiming their data would be leaked.

"We are 99% sure the rest of their 'new victims' are also fake claims (old data for new breaches)," RedSense posted. "So the best thing for them to do would be to delete all other entries from their blog and stop defrauding honest people."

Callow said there certainly have been plenty of cases in the past where ransomware gangs exaggerated their plunder from a victim organization. But this time feels different, he said.

"It is a bit unusual," Callow said. "This is about trying to still affiliates' nerves, and saying, 'All is well, we weren't as badly compromised as law enforcement suggested.' But I think you'd have to be a fool to work with an organization that has been so thoroughly hacked as LockBit has."
