CDW data to be leaked next week after negotiations with LockBit break down

By Connor Jones

Published: 2023-10-06 · Archived: 2026-04-05 21:41:44 UTC

CDW, one of the largest resellers on the planet, will have its data leaked by LockBit after negotiations over the ransom fee broke down, a spokesperson for the cybercrime gang says.

Speaking to *The Register*, the spokesperson, who uses the alias LockBitSupp, implied that during negotiations CDW offered a sum that was so low it insulted the crooks.

"We published them because in the negotiation process a $20 billion company refuses to pay adequate money," the source said.

"As soon as the timer runs out you will be able to see all the information, the negotiations are over and are no longer in progress. We have refused the ridiculous amount offered."

LockBit did not respond to questions relating to what its original ransom demand was or what CDW offered in the negotiations. It also shirked questions concerning the nature of the data stolen and what methods it used to breach the company.

According to the countdown timer on LockBit's victim blog, CDW's files are scheduled to be published in the early hours of the morning on October 11.

CDW has yet to comment on the incident, which appears to have been ongoing since at least September 3, when the company was first posted to LockBit's blog.

The Register has contacted CDW for clarity but the company has not offered a response.

Its automatic email reply reads: "Thank you for contacting CDW. Your inquiry has been received and will be reviewed. Should there be a fit or an interest in engaging further, we will be in touch as soon as possible."

The UK Information Commissioner's Office (ICO) confirmed that it had not received a breach report from CDW.

Cybersecurity analyst and researcher Dominic Alvieri said the company was technically posted to LockBit's blog three times in total. It was originally "flashed" – a tactic involving the quick posting and deletion of a company to encourage a fast response from the victim.

"When deadlines come and go it is a sign the company is negotiating or has at least acknowledged the incident," he said.

"The repost is usually the final stages. The ransoms process can take weeks/months."

Posting a company to a victim blog multiple times isn't something that happens in every case but it is a known aggressive tactic adopted by ransomware groups to hurry negotiations, experts told *The Register*.

"Ransomware groups are ramping up their tactics in forcing victims to pay quickly and this is all part of their business model to extort more money in a timely fashion from their targets," said Jake Moore, global cybersecurity advisor at ESET.

"LockBit has previously used pressure tactics to force other victims of their attacks in order to speed up ransom negotiations to ultimately pay up and with varying success.

"There is always a chance, however, that this is a tactic used to force their victims' hands to act quickly yet no real substance be in the original claim.

"This is the common gamble played between cybercriminals and their victims where one wrong move and a poker face could cost companies huge amounts in ransom payments and more problems thereafter from leaked data in public view."

One historical example of LockBit setting deadlines and not dumping the stolen data was during the attack on Royal Mail International earlier this year.

The deadline was set for February 13 and no data was published. A day later, instead of making Royal Mail International's stolen data public, LockBit posted the full negotiation history between it and the company in the form of a downloadable chat log.

- BYOD should stand for bring your own disaster, according to Microsoft ransomware data
- Feds hopelessly behind the times on ransomware trends in alert to industry
- California passes bill to set up one-stop data deletion shop
- Ransomware fiends pounce on Cisco VPN brute-force zero-day flaw

The chat logs revealed the ransom demand was originally set at $80 million, later offering a 50 percent discount after the company branded the demands "absurd."

At the time, the release of the chat logs was seen as an example of these scare tactics. After Royal Mail's continued refusal to pay, LockBit eventually staggered the publication of its data, much of which included employee information, in 10 separate dumps.

The UK's National Cyber Security Centre (NCSC) has a longstanding stance against paying ransoms to cybercriminals.

In a study by security company CyberEdge, it was found that less than half of businesses paying ransoms recover all of their data.

In the Royal Mail negotiations, the transcript shows the negotiator attempting to convince LockBit to hand over two files as proof the criminals' decryptor worked.

LockBit realized after a few days that the two files would have allowed Royal Mail to fully recover its systems without paying for the decryptor.

Towards the end of the negotiations, where Royal Mail appeared to stall LockBit for as long as it could by saying it was waiting for its board to decide on whether to pay the discounted ransom fee, LockBit grew frustrated with the tactics and published the data after days on non-responsiveness from Royal Mail.

LockBit's lies, and other strange tactics

Over the years, LockBit has been accused of orchestrating various "PR stunts" to cause confusion and raise its notoriety level.

These have included "fake" ransomware attacks on large organizations, posting their details to LockBit's website along with a countdown timer to indicate the publication date of the stolen files, just as it does with genuine victims.

One such example came in June 2022, when it claimed to have breached incident response specialists Mandiant. In typical fashion, the countdown timer spent days reaching zero, and what was published wasn't the data it claimed to have stolen from the company, but instead a response to claims that the group was linked to the sanctioned cybercrime outfit Evil Corp.

"The PR stunt was likely orchestrated by LockBit because an association of their activities to Evil Corp could have financially devastating consequences for their operations," said ReliaQuest in a blog post.

"Paying ransoms to these cyber threat groups is still not illegal in most countries; however, a formalized association with Evil Corp would render those payments potentially out of the law, with significant civil and criminal implications for the organizations involved in them.

"Given that LockBit is one of the most prolific ransomware groups in activity at the moment, it is likely that they intend to continue their highly successful and profitable ransomware operations for the following months."

LockBit repeated the same trick later that year, this time against French multinational IT company Thales. Although in Thales's case, it was only half fibbing.

At the time, Thales's public statements repeatedly denied evidence of an IT intrusion, but on November 10, 2022 – three days after LockBit promised to publish its data – Thales confirmed that data had been stolen and published.

However, it said the theft was carried out by "two likely sources," one of which was "confirmed through the user account of a partner on a dedicated collaboration portal," and the other was unknown. ®
