LockBit brags: We'll leak thousands of SpaceX blueprints stolen from supplier

By Jessica Lyons

Published: 2023-03-13 · Archived: 2026-04-02 11:38:34 UTC

Ransomware gang Lockbit has boasted it broke into Maximum Industries, which makes parts for SpaceX, and stole 3,000 proprietary schematics developed by Elon Musk's rocketeers.

The prolific cybercrime crew also mocked the SpaceX supremo, and threatened to leak or sell on the blueprints from March 20 if the gang's demands to pay up aren't met. This may therefore be a bill Musk can't avoid to reconcile, unlike others, reportedly.

"I would say we were lucky if SpaceX contractors were more talkative. But I think this material will find its buyer as soon as possible," Lockbit posted on its dark-web homepage, according to a screenshot shared on Twitter by security analyst Dominic Alvieri.

We take that broken English to mean Maximum Industries may not be willing to cough up so far, yet the gang believes it may be paid either way: the ransom demand is provided to ensure any stolen files remain unpublished, or someone else will purchase a copy of the data anyway. What's interesting is that the schematics by themselves may not be that useful: you still have to manufacture the parts, which is non-trivial, and then use them without setting off suspicion.

A leak would still be embarrassing, and might attract unwanted attention from the US government – for the crooks and the businesses involved, given the reliance on SpaceX to launch stuff for Uncle Sam.

"Elon Musk, we will help you sell your drawing to other manufacturers — build the ship faster and fly away," the gang continued. It also claimed the 3,000 drawings had been "certified" by SpaceX engineers, but we can't confirm if anyone outside of the ransomware gang has verified the purloined dataset is what it's claimed to be.

Neither SpaceX nor Maximum Industries responded to *The Register*'s calls and emails seeking comment on the reported security breach.

These SpaceX claims follow several others by LockBit-affiliated criminals, which aren't always the most honest bunch about what — if anything — they've stolen.

Last month, the same group of miscreants claimed to have infiltrated financial technology firm ION and threatened to publish stolen data on February 4 if the software provider doesn't pay up. LockBit said the ransom was paid, but they didn't provide any proof and ION declined to comment.

- LockBit's Royal Mail ransom deadline flies by. No data released
- LockBit brags it pumped ION full of ransomware
- Pepsi Bottling Ventures says info-stealing malware swiped sensitive data

- Intruder alert: WH Smith hit by another cyber attack

Meanwhile, another alleged LockBit victim, Royal Mail in the UK, resumed international shipments in February after confirming a "cyber incident" the month prior. Ultimately, the malware slingers appeared to have given up on getting the ransom they asked from Royal Mail before publishing some files they claimed were from the stolen loot.

The UK mail service told Reuters that its investigation didn't find any financial or sensitive customer information among the data the thieves stole. ®

Stop press

As we were going live with this article, the ALPHV ransomware crew claimed it had hit Amazon's doorbell-maker Ring, and was attempting to extort the biz.

A spokesperson for Ring told *The Register* it doesn't believe it was attacked: "We currently have no indications that Ring has experienced a ransomware event."

It's believed a third-party supplier suffered an intrusion of some kind, though, and that this vendor does not have access to Amazon or Ring customer information. The internet giant is working with its supplier regarding this snafu. We'll let you know when we know more – drop us a note if you have any insight to share.
