

## Ransomware attack hits major US data center provider

By Written by Catalin Cimpanu, ContributorContributor Dec. 4, 2019 at 8:08 p.m. PT

Archived: 2026-04-05 12:45:31 UTC



[CyrusOne](#), one of the biggest data center providers in the US, has suffered a ransomware attack, ZDNet has learned.

In an email after this article's publication, a CyrusOne spokesperson confirmed the incident and said they are currently working with law enforcement and forensics firms to investigate the attack, and help customers restore systems impacted systems.

"Six of our managed service customers, located primarily in our New York data center, have experienced availability issues due to a ransomware program encrypting certain devices in their network," CyrusOne told ZDNet.

"Our data center colocation services, including IX and IP Network Services, are not involved in this incident. Our investigation is on-going and we are working closely with third-party experts to address this matter," the company said.

### **Another REvil (Sodinokibi) attack**

According to details ZDNet received in a tip, the incident took place yesterday and was caused by a version of the REvil (Sodinokibi) ransomware.

This is the same ransomware family that hit [several managed service providers](#) in June, [over 20 Texas local governments](#) in early August, and [400+ US dentist offices](#) in late August.

According to a copy of the ransom note, this was a targeted attack against the company's network. The point of entry is currently unknown.



One of the six customers impacted by the ransomware infection is FIA Tech, a financial and brokerage firm. The ransomware caused an outage of FIA Tech cloud services.

[In a message to customers](#), FIA Tech said "the attack was focused on disrupting operations in an attempt to obtain a ransom from our data center provider." FIA Tech did not name the data center provider, but a quick search identifies it as CyrusOne.

We've been told by a source close to CyrusOne that the data center provider does not intend to pay the ransom demand, barring any future unforeseen developments.

The company owns 45 data centers in Europe, Asia, and the Americas, and has more than 1,000 customers. It is also considering a sale after receiving takeover interest over the summer, [according to Bloomberg](#).

CyrusOne is a publicly-traded, NASDAQ-listed company ([NASDAQ:CONE](#)). In an SEC filing last year, the company explicitly listed "ransomware" as a risk factor for its business ([page 23](#)).

A copy of the ransomware executable that is believed to have infected the company's network was [uploaded on VirusTotal](#) earlier today.

*Article updated on December 5, 13:45 ET with comment from CyrusOne.*

**Cloud services: 24 lesser-known web services your business needs to try**

**Security**

---

Source: <https://www.zdnet.com/article/ransomware-attack-hits-major-us-data-center-provider/>