

Green Energy Company Volue Hit by Ransomware

By Eduard Kovacs

Published: 2021-05-13 · Archived: 2026-04-06 02:02:02 UTC

Norway-based green energy solutions provider Volue has been working on restoring systems after being targeted in a ransomware attack.

Volue offers industrial IoT, data and market analysis, power trading, construction software, optimization and trading software, water infrastructure documentation and management, and transition and distribution software solutions to more than 2,200 customers across 44 countries, particularly in Europe. Volue was created in 2020 by combining Powel, Wattsight, Markedskraft and Scanmatic in one international group.

[The attack](#) was discovered on May 5, when Volue said some of its operations had been impacted. The company shut down affected applications and started working on restoring systems. It said all data had been backed up in the cloud and backups were not affected by the attack.

The attack involved the notorious [Ryuk ransomware](#), whose operators make a profit by asking for a ransom after encrypting a company's files. However, they do not appear to operate a website where they leak data stolen from victims who refuse to pay up, a fact that Volue pointed out following the attack. It also noted that Ryuk operators are "not known for performing supply chain attacks."

Cybersecurity firms Digital Shadows and Kaspersky have confirmed for SecurityWeek that Ryuk operators do not appear to be running a leak website. However, Kurt Baumgartner, principal security researcher at Kaspersky, pointed out that this could change at any time.

While there are some code-level similarities between the Ryuk and [Conti](#) ransomware families, they appear to be used by different threat groups that are not connected, Baumgartner said. Conti operators do run a website where they leak data stolen from victims, but Volue is not mentioned there.

Advertisement. Scroll to continue reading.



Is Your VPN a Gateway for Attackers?

2026 VPN Risk Report

[Learn More](#)



After the attack was disclosed, Volue asked customers to log off from its servers to “avoid any further spreading of the ransomware,” and also asked them to change their passwords for Volue services.

Volue’s investigation is ongoing, but so far it has found no evidence of data exfiltration, either personal or “energy-sensitive data.” The firm said the attack targeted systems related to Powel domains, but the Volue domain did not appear to be compromised.

The company said most of its employees had been working from home at the time of the attack and they were not impacted.

“Over the past few days, we have made significant progress and we expect to be fully operational within a few days,” Volue said on Tuesday. “We have a structured process in place to deem safe our customers’ products and services. We continue to see no evidence that customer environments or applications were directly impacted from this attack.”

The ransomware attack on Volue came just days before Colonial Pipeline, the largest refined products pipeline in the United States, said it was [forced to shut down operations](#) due to a ransomware attack.

The attack involved the Darkside ransomware and it had significant implications, including states declaring a state of emergency, temporary gas shortages caused by panicked motorists stocking up over fears of gas shortages caused by the hack, and gas prices rising.

Related: [EDP Renewables North America Discloses Data Breach](#)

Related: [Cisco Firewall Exploited in Attack on U.S. Renewable Energy Firm](#)

Source: <https://www.securityweek.com/green-energy-company-volue-hit-ransomware>