PowerSchool hacker now extorting individual school districts

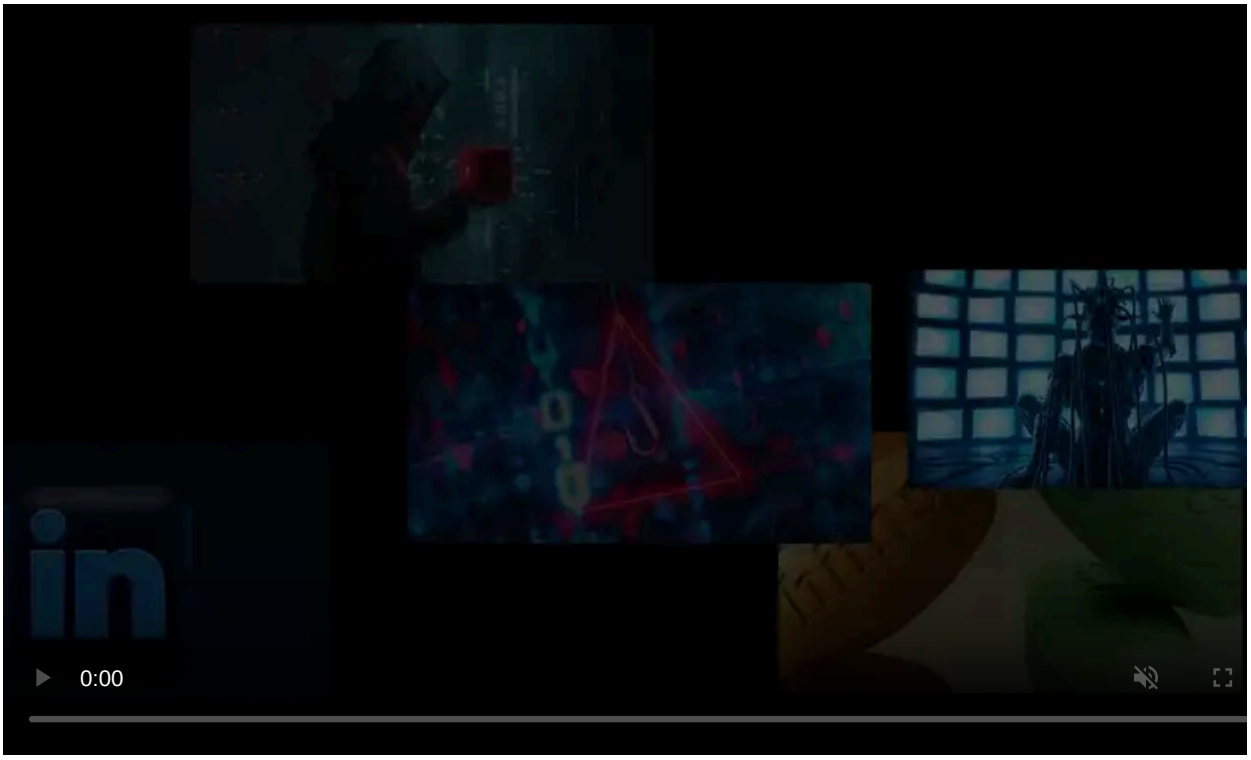
By Lawrence Abrams

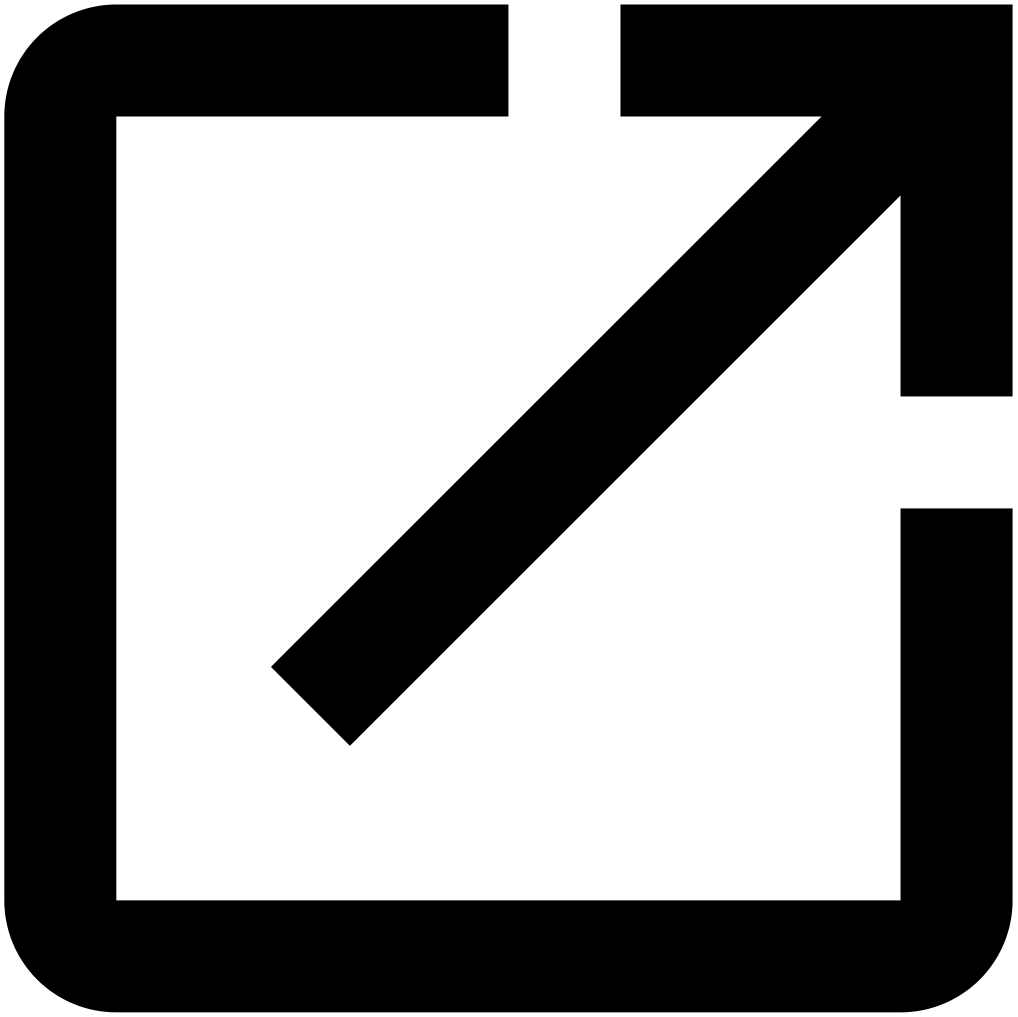
Published: 2025-05-07 · Archived: 2026-04-05 16:50:33 UTC

PowerSchool is warning that the hacker behind its December cyberattack is now individually extorting schools, threatening to release the previously stolen student and teacher data if a ransom is not paid.

"PowerSchool is aware that a threat actor has reached out to multiple school district customers in an attempt to extort them using data from the previously reported December 2024 incident," PowerSchool shared in a statement to BleepingComputer.

"We do not believe this is a new incident, as samples of data match the data previously stolen in December. We have reported this matter to law enforcement both in the United States and in Canada and are working closely with our customers to support them. We sincerely regret these developments – it pains us that our customers are being threatened and re-victimized by bad actors."


0:00



PowerSchool apologized for the ongoing threats caused by the breach and says they will continue to work with customers and law enforcement to respond to the extortion attempts.

The company also recommends that students and faculty take advantage of the free two years of credit monitoring and identity protection to protect against fraud and identity theft. More details about this can be found in the company's security incident FAQ.

PowerSchool also reflected on their choice to pay the ransom demand, stating that it was a difficult decision but hoping it would protect its customers.

"Any organization facing a ransomware or data extortion attack has a very difficult and considered decision to make during a cyber incident of this nature. In the days following our discovery of the December 2024 incident, we made the decision to pay a ransom because we believed it to be in the best interest of our customers and the students and communities we serve," continued the PowerSchool statement.

"It was a difficult decision, and one which our leadership team did not make lightly. But we thought it was the best option for preventing the data from being made public, and we felt it was our duty to take that action. As is always the case with these situations, there was a risk that the bad actors would not delete the data they stole, despite assurances and evidence that were provided to us."

Some of the school districts being individually extorted by the threat actor are those in North Carolina and the Toronto District School Board (TDSB), which is the largest school board in Canada.

"Earlier this week, TDSB was made aware that the data was not destroyed. TDSB, along with other North American school boards, received a communication from a threat actor demanding a ransom using data from the previously reported December 2024 incident," reads a letter to parents.

The PowerSchool data breach

In January, PowerSchool disclosed that it suffered a breach of its PowerSource customer support portal through compromised credentials. Using this access, the threat actors utilized a PowerSource remote maintenance tool to connect to and download the school district's PowerSchool databases.

These databases contained different information depending on the district, including students' and faculty's full names, physical addresses, phone numbers, passwords, parent information, contact details, Social Security numbers, medical data, and grades.

The breach was initially detected on December 28, 2024, but the company later revealed that it was breached months earlier, in August and September 2024, using the same compromised credentials.

As first reported by BleepingComputer, the hacker claimed to have stolen the data of 62.4 million students and 9.5 million teachers for 6,505 school districts across the U.S., Canada, and other countries.

In a FAQ only accessible to customers and seen by BleepingComputer at the time, PowerSchool confirmed that they paid a ransom to prevent the data from being released and received a video from the threat actor claiming the data had been deleted. However, it appears now that the threat actor did not keep their promise.

Security experts and ransomware negotiators have long advised against companies paying a ransom to prevent the leaking of data, as threat actors are increasingly failing to keep their promise to delete stolen data.

Unlike a decryption key, which companies can confirm works, there is no way to adequately verify that data is deleted as promised.

This was recently seen in UnitedHealth's Change Healthcare ransomware attack, in which they paid a ransom to the BlackCat ransomware gang to receive a decryptor and not leak data.

However, after BlackCat pulled an exit scam, the affiliate behind the attack said they still had the data and extorted UnitedHealth once again.

It is believed that UnitedHealth paid a second ransom to once again prevent the leaking of the data.

Update 5/7/25: Added some of the districts being individually extorted.

Source: https://www.bleepingcomputer.com/news/security/powerschool-hacker-now-extorting-individual-school-districts/