BLACKSWAN CYBERSECURITY

THREAT ADVISORY

May 8, 2025

Targeted Extortion of School Districts Following PowerSchool Breach

EXECUTIVE SUMMARY

Blackswan Cybersecurity is actively monitoring the evolving threat landscape following the PowerSchool breach initially detected in December 2024. Recent developments indicate that the threat actor responsible for the incident is now individually extorting K-12 school districts, leveraging data exfiltrated during the original breach. Despite PowerSchool's efforts—including the payment of a ransom and collaboration with law enforcement—affected school systems continue to face re-victimization. This report outlines the sequence of events, threat actor tactics, implications for the education sector, and critical guidance for prevention and response.

INCIDENT OVERVIEW

In December 2024, PowerSchool detected unauthorized access to its PowerSource customer support portal. The breach, traced back to compromised credentials, enabled the attacker to use a remote maintenance tool to exfiltrate sensitive school district data from across the U.S., Canada, and other regions. According to threat actor claims, the data set includes information on over 62 million students and 9.5 million teachers across 6,505 school districts.

PowerSchool later confirmed the breach originated months earlier, in August and September 2024. Despite responding by paying a ransom and receiving a purported deletion video from the attacker, the threat actor has now resumed extortion attempts—this time targeting individual school districts directly.

CURRENT THREAT ACTIVITY: TARGETED EXTORTION

PowerSchool has issued a statement acknowledging that multiple school district customers are receiving direct extortion threats. The threat actor is demanding separate ransoms under the threat of publishing sensitive student and staff data.

The **Toronto District School Board (TDSB)**—Canada's largest school board—is among the entities receiving extortion communications. A letter to parents from TDSB confirmed that the attacker has retained the stolen data despite previous assurances, indicating a betrayal of the ransom agreement originally made with PowerSchool.

DATA COMPROMISED

The breached databases contain varying levels of sensitive information depending on the school district. The following categories of data are confirmed to be at risk:

- Full names of students and staff
- Physical addresses and phone numbers
- Passwords and login credentials
- Parent/guardian contact details
- Social Security Numbers (SSNs)
- Medical and health-related information
- Academic records and grades

This type of data poses substantial identity theft, social engineering, and fraud risks, especially within vulnerable populations like students and minors.

POWERSCHOOL'S RESPONSE

PowerSchool has reiterated its regret for the continued victimization of its clients and is collaborating with law enforcement agencies in both the United States and Canada. The company has offered two years of complimentary credit monitoring and identity protection services to affected users.

The firm justified its original ransom payment as a difficult but necessary action to protect the students and communities it serves. However, the incident underscores the inherent risk in trusting ransomware actors to uphold their commitments after payment is rendered.

IMPLICATIONS FOR THE EDUCATION SECTOR

This incident highlights several persistent challenges in the K12 cybersecurity ecosystem:

- **High-Value Targets**: Education systems remain lucrative for cybercriminals due to the breadth and sensitivity of personal data they store.
- **Credential Abuse**: The initial compromise through stolen credentials reinforces the need for robust identity and access management (IAM) protocols.
- **Inefficacy of Ransom Payments**: Paying ransom does not guarantee that data will be deleted or withheld from public release. This case mirrors broader industry trends, such as the Change Healthcare and UnitedHealth incidents, where paid ransoms failed to prevent continued extortion.

BLACKSWAN'S RECOMMENDATIONS

Blackswan Cybersecurity urges school districts, education service providers, and technology vendors to take immediate action:

1. Zero Trust Architecture

Adopt a zero-trust framework to limit lateral movement and restrict access based on verified identity and device posture.

2. Credential Hygiene and MFA

Enforce multi-factor authentication (MFA) across all privileged accounts and conduct routine credential audits.

3. Threat Detection and Response

Implement Managed Detection and Response (MDR) services to monitor and neutralize threats before data can be exfiltrated.

4. Data Minimization and Segmentation

Reduce unnecessary data retention and apply strict network segmentation to isolate sensitive records.

5. Incident Response Preparedness

Maintain a tested incident response plan, inclusive of extortion scenarios, communications strategies, and legal considerations.

BLACKSWAN CYBERSECURITY: TRUSTED PROTECTION FOR K12

With over a decade of defending educational institutions, Blackswan Cybersecurity remains a frontline partner to schools nationwide. Our 24/7 Cyber Fusion Center, Open XDR platform, and expert vCISO services have helped districts mitigate attacks like this before they escalate. We remain committed to safeguarding the digital trust of students, educators, and their communities.

To schedule a threat briefing or discuss hardening your district's security posture, contact us at: contact@blackswancybersecurity.com or blackswan-cybersecurity.com.

REFERENCES

- https://www.bleepingcomputer.com/news/security/powerschool-hacker-now-extorting-individual-school-districts/
- https://www.nbcnews.com/tech/security/school-districts-hit-extortion-attempts-powerschool-breach-rcna205429
- https://therecord.media/despite-ransom-payment-powerschool-extorting