Securin

The PowerSchool Breach

What you need to know about cyber attacks on education.

What Happened?

Attackers gained access to PowerSchool's support platform, PowerSource, using compromised credentials. From there, they exploited a maintenance tool designed for engineers, gaining access to customer Student Information System (SIS) instances. Student and teacher databases were exfiltrated. PowerSchool paid a ransom to the attackers, in return for assurances that the stolen data would be destroyed and not disseminated.

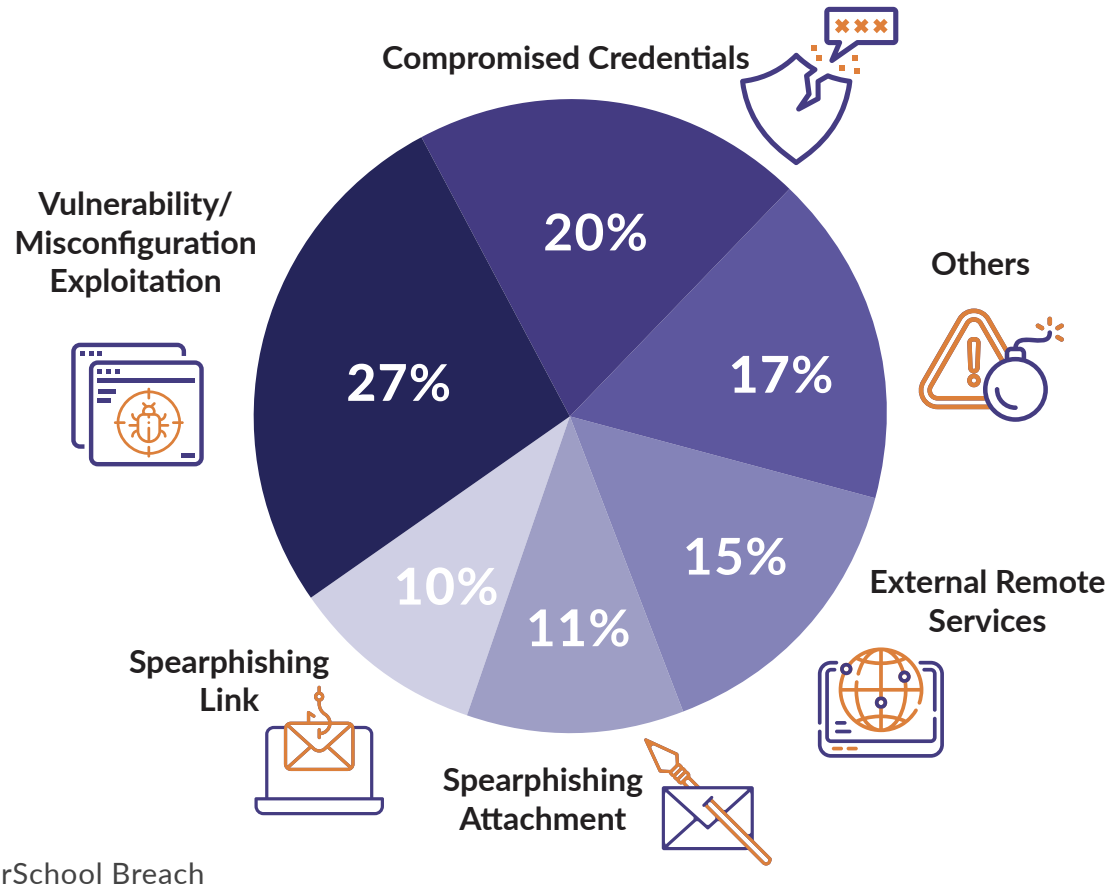
PowerSchool

- **K-12 EduTech Company**
- **60 Million+ Students Served Worldwide**
- **Breach Technique:**
  - Compromised Credentials
  - Exploitation of Maintenance Tools
- **Potential Impact:**
  - Sensitive Data like SSN
  - Contact Details

Key Attack Vectors in Education

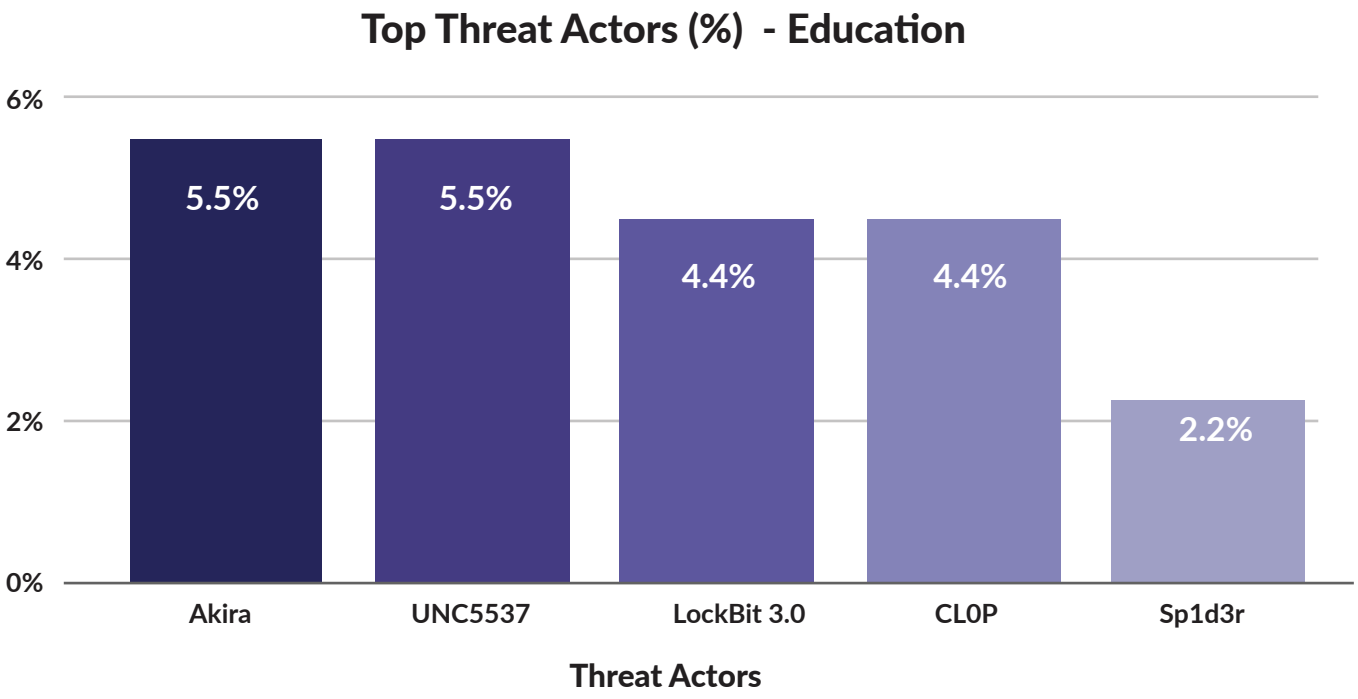
The PowerSchool attack comes at a time when schools are under increasing pressure to protect their networks and sensitive data about students and staff. Securin's analysis of over 230 education sector attacks in the past year indicates that compromised credentials and vulnerability/misconfiguration exploits together account for almost half of initial access vectors in attacks. From a defense perspective, both are considered 'low hanging fruit' in theory, if not always in practice.

Initial Access Vectors Distribution (%) - Education



Who's Attacking Education?

The top threats targeting the education sector are from criminal / ransomware gangs, including:



Threat Actor

Akira: Since 2023, this ransomware group rapidly became a significant threat. By January 2024, Akira had compromised over 250 organizations, including Stanford University and Carnegie Mellon, extorting over $42 million in ransom payments.

MO: Vulnerabilities in VPN services - particularly ones lacking multi-factor authentication (MFA) - are a favoured route for initial access, along with compromised credentials. Once inside, Akira moves laterally, escalating privileges to gain control, exfiltrate data or encrypt it.

Threat Actor

UNC5537: Known for targeting cloud-based data storage and analytics platforms (including the high-profile Snowflake breach). This group focuses on rapid data exfiltration from high-value targets.

MO: For initial access, UNC5537 uses stolen credentials gained from malware/infostealer campaigns. Once inside, they collect user and system information, using SQL queries to gather and exfiltrate data, which is used for extortion or sold on the dark web.

Threat Actor

Lockbit 3.0: Responsible for an estimated 44% of all ransomware attacks globally in 2023, the group claims to be "Completely apolitical, and only interested in money."

MO: Lockbit's favored initial access methods include exploiting public-facing applications, weak passwords / lack of MFA, phishing, and remote desktop protocol (RDP). It has been known to exploit CVEs in widely used products including Microsoft Windows Server and Exchange.

Why is This Happening?

As organizations continue to collect massive amounts of data – often more than is actually needed – the risk of high-impact breaches increases exponentially. Even with robust regulations such as GDPR, HIPAA and CCPA in place, there's a clear need to refine controls around limiting the data collected, and ensuring it's properly safeguarded.

> **"As data breaches become more common, you're likely right in assuming that your data has been compromised in some way by now."**
>
> **- Kiran Chinnagangannagari, Secuirn Chief Product & Technology Officer**

What Can You Do To Mitigate The Risks?

Securin's Kiran Chinnagangannagari says that, from the vendor perspective, MFA and CISA's Secure-by-Design factors should be default practices. At the individual level, basic cybersecurity hygiene such as monitoring for compromised accounts and MFA will help – but the reality is, we're all walking around with potentially compromised information, from our social security numbers to children's data. "We need to balance stronger regulatory insight with practical, everyday security practices."

Stay Secure with this Cyber Hygiene Checklist

- [ ] Enable MFA wherever possible to add an extra layer of security.
- [ ] Keep all software and devices up to date with the latest security patches.
- [ ] Practice caution about sharing personal information online.
- [ ] Avoid clicking on suspicious links or unknown sources.
- [ ] Choose strong passwords and change them regularly.
- [ ] Be proactive in adopting security measures.



About Securin

At Securin, we empower teams and organizations to minimize their business risk with our comprehensive range of offensive cybersecurity solutions. These solutions are carefully crafted to be intuitive, adaptable, and scalable, catering to organizations of all sizes in today's ever-changing digital landscape. Securin's human-augmented intelligence approach to cybersecurity empowers organizations to thrive by proactively addressing emerging threats and uncertainties, ensuring their security.

Securin
securin.io

Follow Us On