kaspersky bring on the future

Report

Ransomware attacks on K-12 schools

Parents report more attacks, longer closures, higher ransoms

In October 2022, Kaspersky surveyed 2,000 parents of school-age children in the United States to find out how many have experienced ransomware attacks on their schools, how the attacks affected the victims and how the schools responded. The results are compared to a previous report that posed the same questions to a similar group of parents in October 2021, as well as to an earlier report in May 2021 asking parents more generally about cyberattacks on schools.

Key findings

- **14%** of parents said their child's school has been **hit with a ransomware attack while** they were a student there. This was up from 9% in October 2021.
- Parents reporting an attack said their school district paid an average ransom of **$887,360** to the attackers. In 2021, the figure was just $375,311.
- 82% of parents reporting attacks said their school was forced to close for at least 1 day, up from 75% in October 2021. The **average closure was 2.5 days**, up slightly from 2.3 days reported last year.

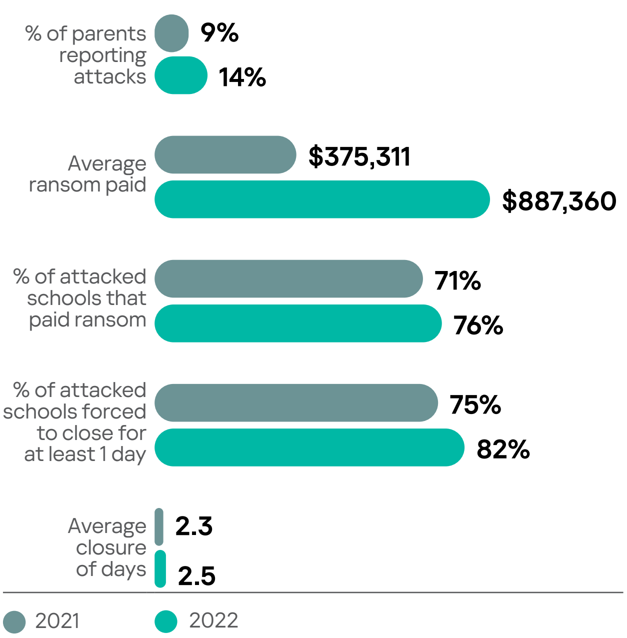
The Impact

- 60% of parents reporting an attack said their child's data was compromised (61% in 2021), while 32% said it was not compromised. This was up from 25% in October 2021.
- 10% of parents reporting an attack said the district paid a ransom of more than $1M; up from 3.7% in 2021.
- 32% of affected parents said they were notified by the school immediately; down slightly from 34% in the May 2021 survey.
- 82% of parents were satisfied with their school's response to the attack, up from 80% in October 2021.
- 69% of all parents said they talk at least regularly with their child about practicing good security hygiene, such as using strong passwords, down from 75% in May 2021.
- 81% of all parents said they are confident in their school's ability to successfully handle cybersecurity incidents in the future. In May 2021, only 68% said they think their school was somewhat or very prepared for an attack.

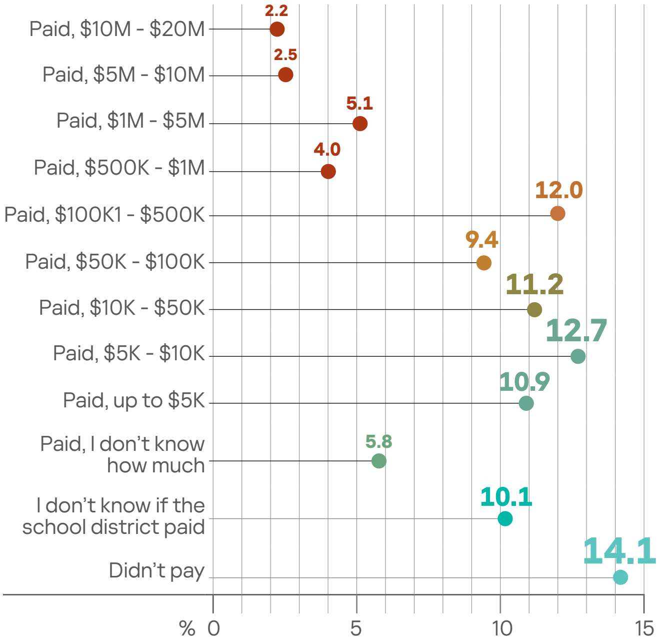
> “This fall, cybercriminals continued to attack vulnerable schools in an effort not only to get ransom money, but also to steal students’ and teachers’ Social Security numbers, banking information, and even medical histories. It is, however, encouraging to see that a growing number of schools appear to be protecting student data. We urge school administrators to build on this success by employing some basic security mechanisms, such as multi-factor authentication, regular software updates and training staff and students to spot phishing attacks. No one should ever pay a ransom, which continues to perpetuate the problem.”

Kurt Baumgartner,
principal security researcher,
Kaspersky

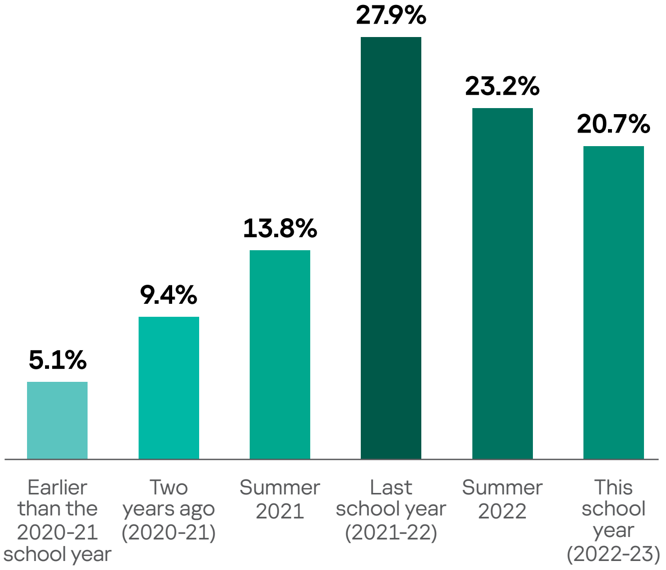
Attacks, ransoms and closures on the rise



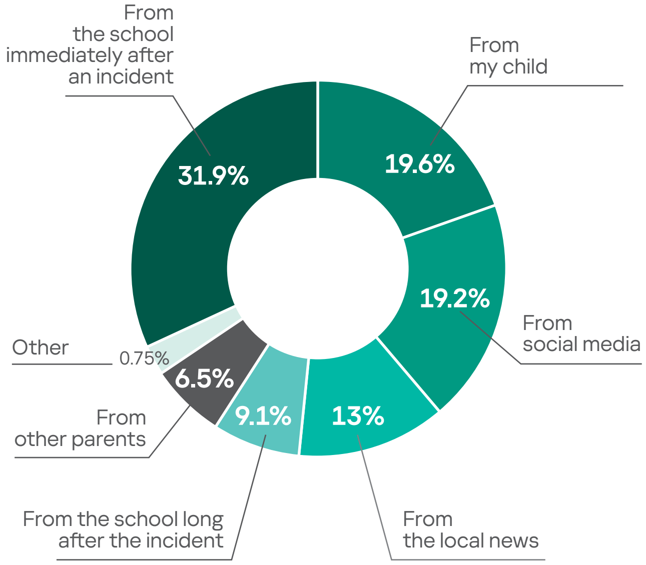
Ransom payments



When the attacks occurred



How parents were notified



kaspersky.com

Reference links:

Last year’s data is available in this Ransomware Attacks on K-12 Schools report
Additional data and safety tips for parents, students and educators are available in this June 2021 survey report.