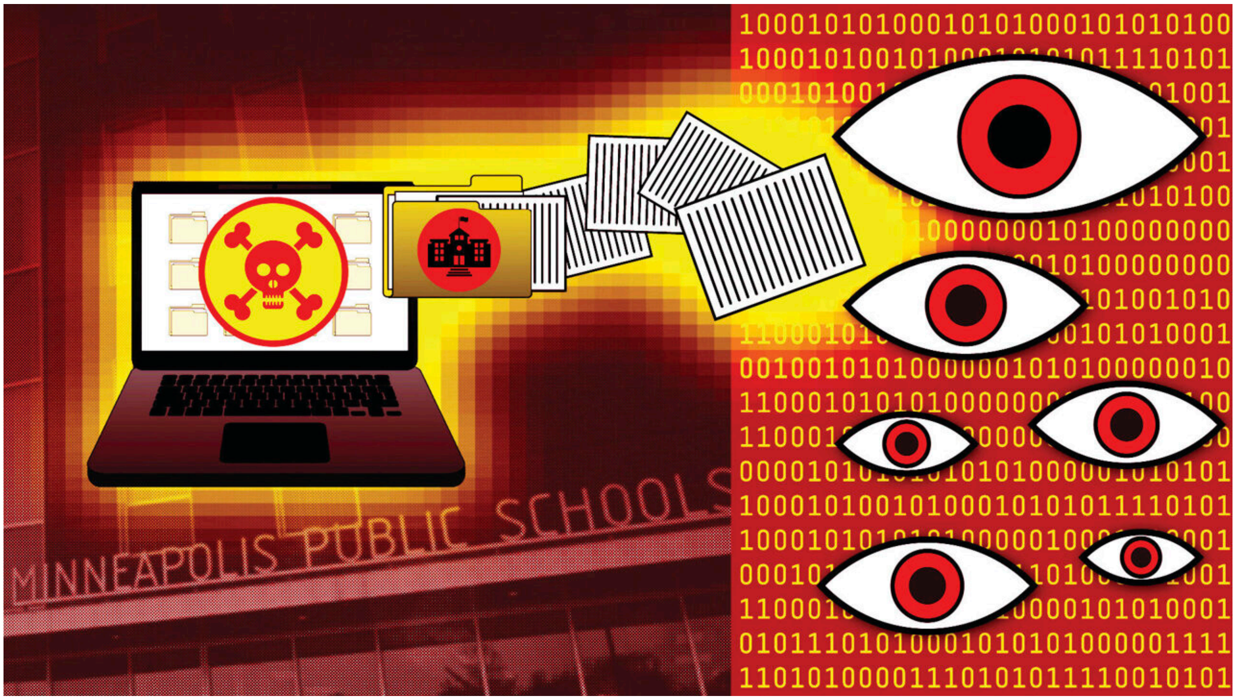
TechXplore

Ransomware criminals are dumping kids' private files online after school hacks

July 5 2023, by FRANK BAJAK, HEATHER HOLLINGSWORTH and LARRY FENN



Credit: AP Illustration/Peter Hamlin

The confidential documents stolen from schools and dumped online by ransomware gangs are raw, intimate and graphic. They describe student sexual assaults, psychiatric hospitalizations, abusive parents, truancy—even suicide attempts.

"Please do something," begged a student in one leaked file, recalling the trauma of continually bumping into an ex-abuser at a school in Minneapolis. Other victims talked about wetting the bed or crying themselves to sleep.

Complete sexual assault case folios containing these details were among more than 300,000 files dumped online in March after the 36,000-student Minneapolis Public Schools refused to pay a $1 million ransom. Other exposed data included medical records, discrimination complaints, Social Security numbers and contact information of district employees.

Rich in digitized data, the nation's schools are prime targets for far-flung criminal hackers, who are assiduously locating and scooping up sensitive files that not long ago were committed to paper in locked cabinets. "In this case, everybody has a key," said cybersecurity expert Ian Coldwater, whose son attends a Minneapolis high school.

Often strapped for cash, districts are grossly ill-equipped not just to defend themselves but to respond diligently and transparently when attacked, especially as they struggle to help kids catch up from the pandemic and grapple with shrinking budgets.

Months after the Minneapolis attack, administrators have not delivered on their promise to inform individual victims. Unlike for hospitals, no federal law exists to require this notification from schools.

The Associated Press reached families of six students whose sexual assault case files were exposed. The message from a reporter was the first time anyone had alerted them.

"Truth is, they didn't notify us about anything," said a mother whose son's case file has 80 documents.

Even when schools catch a ransomware attack in progress, the data are typically already gone. That was what Los Angeles Unified School District did last Labor Day weekend, only to see the private paperwork of more than 1,900 former students—including psychological evaluations and medical records—leaked online. Not until February did district officials disclose the breach's full dimensions, noting the complexity of notifying victims with exposed files up to three decades old.

The lasting legacy of school ransomware attacks, it turns out, is not in school closures, recovery costs or even soaring cyberinsurance premiums. It is the trauma for staff, students and parents from the online exposure of private records—which the AP found on the open internet and dark web.

"A massive amount of information is being posted online, and nobody is looking to see just how bad it all is. Or, if somebody is looking, they're not making the results public," said analyst Brett Callow of the cybersecurity firm Emsisoft.

Other big districts recently stung by data theft include San Diego, Des Moines and Tucson, Arizona. While the severity of those hacks remains unclear, all have been criticized either for being slow to admit to being hit by ransomware, dragging their feet on notifying victims—or both.

ON CYBER SECURITY, SCHOOLS HAVE LAGGED

While other ransomware targets have fortified and segmented networks, encrypting data and mandating multi-factor authentication, school systems have been slower to react.

Ransomware likely has affected well over 5 million U.S. students by now, with district attacks on track to rise this year, said analyst Allan Liska of the cybersecurity firm Recorded Future. Nearly one in three U.S. districts had been breached by the end of 2021, according to a survey by the Center for Internet Security, a federally funded nonprofit.

"Everyone wants schools to be more secure, but very few want to see their taxes raised to do it," Liska said.

Parents have instead pushed to use limited funds on things like bilingual teachers and new football helmets, said Albuquerque schools superintendent Scott Elder, whose district suffered a January 2022 ransomware attack.

Just three years ago, criminals did not routinely grab data in ransomware attacks, said TJ Sayers, cyberthreat intelligence manager at the Center for Internet Security. Now, it's common, he said, with much of it sold on the dark web.

The criminals in the Minneapolis theft were especially aggressive. They shared links to the stolen data on Facebook, Twitter, Telegram and the dark web, which standard browsers can't access. A handwritten note naming three students involved in one of the sexual abuse complaints was featured for a time on YouTube competitor Vimeo, which promptly took down the video.

The cybercrime syndicate behind the Los Angeles United attack was less brazen. But the 500 gigabytes it dumped on its dark web "leak site" remained freely available for download in June. They include financial records and personnel files with scanned Social Security cards and passports.

The public disclosure of psychological records or sexual assault case files, complete with students' names, can fray psyches and thwart careers, psychologists say. One file stolen from Los Angeles United described how a middle-schooler had attempted suicide and been in and out of the psychiatric hospital a dozen times in a year.

Credit: AP Illustration/Peter Hamlin

The mother of a 16-year-old with autism recently got a letter from the San Diego Unified School District saying her daughter's medical records may have been leaked online in an Oct. 25 breach.

"What," Barbara Voit asked, "if she doesn't want the world to know that she has autism?”

IN A TRICKLE, THE EXTENT OF A BREACH

EMERGES

The Minneapolis parents informed by the AP of the leaked sexual assault complaints feel doubly victimized. Their children have battled PTSD, and some even left their schools. Now this.

"The family is beyond horrified to learn that this highly sensitive information is now available in perpetuity on the internet for the child's future friends, romantic interests, employers, and others to discover," said Jeff Storms, an attorney for one of the families. It is AP policy not to identify sexual abuse victims.

Teachers, meanwhile, want to know why they have to call the district and report problems in order to receive the promised free credit monitoring and identity theft protection after their Social Security numbers were leaked.

"Everything they've learned about this is from the news," said Greta Callahan, of the Minneapolis Federation of Teachers.

Minneapolis Schools spokeswoman Crystina Lugo-Beach would not say how many people have been contacted so far or answer any other AP questions about the attack.

School nurse Angie McCracken had by early April already received 10 alerts through her credit card that her Social Security number and birth date were circulating on the dark web. She wondered about her graduating 18-year-old. "If their identity is stolen, just how hard is that going to make my kid's life?"

Despite parents' and teachers' frustration, schools are routinely advised by incident response teams concerned about legal liability issues and ransom negotiations against being more transparent, said Callow of

Emsisoft. Minneapolis school officials apparently followed that playbook, initially describing the Feb. 17 attack cryptically as a "system incident," then as "technical difficulties" and later an "encryption event."

The extent of the breach became clear though when a ransomware group posted video of stolen data more than two weeks later, giving the district 10 days to pay the ransom before leaking files.

The district declined to pay, following the standing advice of the FBI, which says ransoms encourage criminals to target more victims.

SCHOOLS SPEND TECH BUDGETS ON LEARNING TOOLS, NOT SECURITY

During the COVID-19 pandemic, districts prioritized spending on internet connectivity and remote learning. Security got short shrift as IT departments invested in software to track student engagement and performance, often at the expense of privacy and safety, University of Chicago and New York University researchers found.

In a 2023 survey, the Consortium for School Networking, a tech-oriented nonprofit, found just 16% of districts had full-time network security staff, with nearly nearly half devoting 2% or less of their IT budgets to security.

With a deficit in private sector cybersecurity talent, districts struggle to hang onto it. Districts who do hire someone often see them snatched away by businesses that can double their salaries, said Keith Krueger, CEO of the consortium.

Cybersecurity money for public schools is limited. As it stands, districts can only expect slivers of the $1 billion in cybersecurity grants that the federal government is distributing over four years.

Minnesota's chief information security officer, John Israel, said his state got $18 million of it this year to divvy among 3,600 different entities, including cities and tribal governments. State lawmakers provided an additional $22.5 million in grants for cyber and physical security in schools.

Schools also want to tap a federal program called E-Rate that is designed to improve broadband connections to schools and libraries. More than 1,100 wrote the Federal Communications Commission after the Los Angeles Unified breach asking that E-Rate be modified to free up funds for cybersecurity. The FCC is still considering the request.

It's already too late for the mother of one of the Minneapolis students whose confidential sexual assault complaint was released online. She almost feels "violated again."

"All the stuff we kept private," she said, "it's out there. And it's been out there for a very long time."

Citation: Ransomware criminals are dumping kids' private files online after school hacks (2023, July 5) retrieved 8 May 2024 from https://techxplore.com/news/2023-07-ransomware-criminals-dumping-kids-private.html