Huge Los Angeles Unified School district hit by cyberattack

September 6 2022, by STEFANIE DAZIO, FRANK BAJAK and ZEKE MILLER

Alberto Carvalho, Superintendent, Los Angeles Unified School District, the nation's second-largest school district, comments on an external cyberattack on the LAUSD information systems during the Labor Day weekend, at a news conference in Los Angeles Tuesday, Sept. 6, 2022. Despite the ransomware attack, schools in the nation's second-largest district opened as usual Tuesday morning. Credit: AP Photo/Damian Dovarganes

A ransomware attack targeting the huge Los Angeles school district prompted an unprecedented shutdown of its computer systems as schools increasingly find themselves vulnerable to cyber breaches at the start of a new year.

The attack on the Los Angeles Unified School District sounded alarms across the country, from urgent talks with the White House and the National Security Council after the first signs of ransomware were discovered late Saturday night to mandated password changes for 540,000 students and 70,000 district employees.

Though the attack used technology that encrypts data and won't unlock it unless a ransom is paid, in this case the district's superintendent said no immediate demand for money was made and schools in the nation's second-largest district opened as scheduled on Tuesday.

Such attacks have become a growing threat to U.S. schools, with several high-profile incidents reported since last year as pandemic-forced reliance on technology increases the impact. And ransomware gangs have in the past planned major attacks on U.S. holiday weekends, when they know IT staffing will be thin and security experts relaxing.

While it was not immediately clear when the LA attack began—officials have only said when it was detected and a district spokesperson declined to answer additional questions—Saturday night's discovery reached the highest levels of the federal government's cybersecurity agencies.

According to a senior administration official, this pattern of support was consistent with the Biden administration's efforts to provide maximum assistance to critical industries affected by such breaches.

The official, who spoke on the condition of anonymity to discuss the federal response, said the school district did not pay ransom, but would

not get into detail on what potentially might have been stolen or damaged and what systems were affected by the breach.

The White House's response to the LA incursion reflects a growing national security concern: A Pew Research Center survey, published last month, found that 71% of Americans say cyberattacks from other countries are a major threat to the U.S.

Authorities believe the LA attack originated internationally and have identified three potential countries where it may have come from, though LA Superintendent Alberto Carvalho would not say which countries may be involved. Most ransomware criminals are Russian speakers who operate without interference from the Kremlin.

LA officials did not identify the ransomware used.

"This was an act of cowardice," said Nick Melvoin, the school board vice president. "A criminal act against kids, against their teachers and against an education system."

So far this year, 26 U.S. school districts—including Los Angeles—and 24 colleges and universities have been hit by so-called ransomware, according to Brett Callow, a ransomware analyst at the cybersecurity firm Emsisoft.

With victims increasingly refusing to pay to have their data unlocked, many cybercriminals instead use the same technology to steal sensitive information and demand extortion payments. If the victim doesn't pay, the data gets dumped online.

Callow said at least 31 of the schools hit this year had data stolen and released online, and noted that eight of the school districts have been hit since Aug. 1. The upsurge on schools as summer vacations end is almost

certainly not coincidental, he said.

"It is the No. 1 threat to our safety," said Michel Moore, chief of the Los Angeles Police Department. "It is an invisible foe and it is tireless."

Tireless—and expensive, even outside of any monetary demands. A ransomware extortion attack in Albuquerque's biggest school district forced schools to close for two days in January, while Baltimore City's response to a 2019 hit on its computer servers cost upwards of $18 million.

The LA attack was discovered around 10:30 p.m. Saturday when staff first detected "unusual activity," Carvalho said. The perpetrators appear to have targeted the facilities systems, which involves information about private-sector contractor payments—which are publicly available through records requests—rather than confidential details like payroll, health and other data.

He said district IT officials detected the malware and stopped it from propagating but not until after it infected key network systems, necessitating the reset of passwords for all staff and students.

Authorities scrambled to trace the intruders and restrict potential damage.

"We basically shut down every one of our systems," Carvalho said, noting that each one had been checked and all but one—the facilities system—restarted by late Monday night, when the district first notified the public of the hit.

On Tuesday, federal authorities separately warned of potential ransomware attacks by the criminal syndicate known as Vice Society, which has allegedly disproportionately targeted the education sector.

Authorities have not said whether they believe Vice Society is involved in the LA attack and the group did not respond to a request for comment on Tuesday.

"The fact that a joint cybersecurity advisory relating to Vice Society was issued within days of the attack on LAUSD being discovered may be telling, especially as this gang has frequently targeted the education sector in both the U.S. and the U.K.," said Callow, the ransomware expert.

Vice Society first appeared in May 2021 and, rather than a unique variant, it has used ransomware widely available in the Russian-speaking underground, security researchers say. Among victims claimed by Vice Society are the Elmbrook School district in Wisconsin and the Savannah College of Art and Design.

Ransomware gangs routinely dissolve after high-profile attacks such as last year's Colonial Pipeline incident, which triggered runs on gas stations. Their members then reconstitute under new names.

While there was pressure to cancel school in Los Angeles on Tuesday, officials ultimately decided to stay open.

Had the activity not been discovered on Saturday night, Carvalho said there could have been "catastrophic" consequences.

"If we had lost the ability to run our school buses, over 40,000 of our students would not have been able to get to school, or it would have been a highly disrupted system," he said.

The district plans to do a forensic audit of the attack to see what can be done to prevent future incursions.

"Every teacher, every employee, every student can be a weak point," said Soheil Katal, the district's chief information officer.