LA Unified cyberattackers demand ransom

September 21 2022, by Howard Blume

Credit: CC0 Public Domain

The hackers who targeted the Los Angeles Unified School District have made a ransom demand, officials confirmed Tuesday, an indication that the attackers have extracted sensitive data or believe they can bluff the district into thinking that they have.

"We can confirm that there was a demand made," L.A. schools Superintendent Alberto Carvalho said. "There has been no response to the demand."

Carvalho declined to disclose the amount of the ransom demand or any further information about what information, if any, the attackers may be holding.

He said that there have been "no new security breaches" and that the school system is continuing "our ramping up of apps and systems."

Officials said they are optimistic that Social Security numbers and other sensitive information of employees remain secure. But the outlook could be different related to student information, such as grades, course schedules, disciplinary records and disability status. The district does not collect Social Security numbers for students and parents.

Earlier Carvalho disclosed that the attackers extended their deadline for entering into negotiations without specifically mentioning a ransom amount. The district, Carvalho added, is following the advice of experts and law enforcement, which includes the FBI as well as the Los Angeles Police Department.

In a related development, federal officials on Friday announced a new major grant program to help public agencies better secure themselves from cyberattack.

The demand for money was widely anticipated in the wake of the cyberattack, which was discovered in progress on the night of Sept. 3, the Saturday of Labor Day weekend.

Hackers will typically threaten to post sensitive data online if they are not paid, but it can be difficult to determine what they've obtained, and

they might be lying.

In general, such payments are a bad idea, said Clifford Neuman, director of USC's Center for Computer Systems Security.

"It is important for any organization impacted by ransomware to understand that even if they pay a ransom demand, they will still incur significant IT expense and delays to repair the system," Neuman said. "The best action is not to pay the ransom and recover systems from backups."

He added: "There is no reason to believe that the criminals would actually delete the exfiltrated data even if the ransom is paid."

The attempted theft of data was one element of the attack on L.A. Unified. The other involved attempting to disable district computer systems, making them inaccessible.

Although both elements of the attack were only partly successful, full recovery has been difficult. The information for a Board of Education meeting Tuesday, for example, was posted via a temporary, cumbersome webpage. Campuses reopened as scheduled on the Tuesday after Labor Day, but many students, parents and staff said a full instructional week was lost as technicians double-checked and gradually rebooted systems and as users reset more than 600,000 passwords.

Along the way, the district discovered malware the attackers left behind, which had the potential to cause more damage if not discovered and carefully disabled.

Carvalho described the malware as "digital tripwires left behind that if tripped will further disable or infect systems." This discovery caused a delay in the reset of district passwords, partly over concerns that the new

passwords could then be stolen as well.

Operations unfolded more smoothly the second week after the attack, although technicians still are trying to restore the online system through which L.A. Unified handles purchases and the bidding process for vendors and construction projects.

Although a recent audit pointed out gaping flaws in the district's online security, L.A. Unified is far from alone.

"The only unusual thing about this attack is that it involved the nation's second-largest school district. That fact aside, incidents such as this are unfortunately all too common," said Brett Callow, threat analyst for Emsisoft, a cybersecurity firm. "Already this year, 25 others districts with 425 schools between them have found themselves in the same position as LAUSD."

Most of those incidents resulted in stolen data being leaked online.

A site that tracks cyberattacks reported that a county office of education in California recently paid a $400,000 ransom.

The L.A. Unified attack has been linked to a criminal syndicate that calls itself Vice Society, although authorities have declined to confirm it.