Hackers penetrated LAUSD computers much earlier than previously known, district probe finds

January 23 2023, by Howard Blume

Credit: Unsplash/CC0 Public Domain

An intrusion into the computer systems of the Los Angeles school district began more than a month earlier than previously disclosed and

likely exposed confidential information, including Social Security numbers, of more than 500 people who worked for district contractors, according to information filed with the state.

As the district previously disclosed, the security breach does not appear to extend to the payroll records and Social Security numbers for the tens of thousands of district employees. An undisclosed number of students enrolled at some point from 2013 through 2016 and some employees during that period appear to have lost information that includes their date of birth and address. California school districts don't collect student Social Security numbers.

The updated information comes by way of a "Notice of Data Breach" that the nation's second-largest school system was required under state law to send to potential victims.

School district officials Friday did not provide information on the number of possible victims. In addition to having to notify victims, a notice letter must be filed with the state attorney general when the number of those affected surpasses 500 California residents, the mandated threshold for public notification.

District officials had previously stated that there would be a small but not-yet-determined number of victims—"outliers," as Supt. Alberto Carvalho described them. The victims would be notified and assisted, he added, while emphasizing that the overriding narrative was one of a worse disaster averted.

Hackers made off with about 500 gigabytes of data—a figure agreed on by both the hackers and the school system. That's a large haul compared with what an individual user would maintain, but a tiny fraction of the data under the control of L.A. Unified.

Stealing data is only one part of an attack. The second part involves encrypting computer systems so that its users cannot get in, paralyzing the ability to conduct everyday business. Hackers managed to encrypt servers in the district's facilities division, but had limited success elsewhere, even though normal operations, including classroom instruction and record-keeping, were more difficult for about two weeks. Schools never had to be temporarily closed—which has happened elsewhere when some school systems were attacked.

L.A. Unified refused to pay a ransom and hackers responded by releasing the data they had onto the dark web, where other bad actors could use it for such purposes as identify theft.

District officials have for months publicly characterized the attack as beginning and ending on Sept. 3—the Saturday of the Labor Day weekend. District technicians, when they noticed the attack, moved quickly and with substantial success to limit its scope.

"In a very, very unique way, we stopped the attack midstream," Carvalho said at a news conference in October. "That's very unusual. What usually happens is the entity finds out about the attack after the information was captured, uploaded, and the servers the system [are] encrypted. ... I can tell you that there have been a number of systems in this country who have fallen victim to this same actor that were not so lucky."

The follow-up investigation determined that an intrusion began as early as July 31.

"Between July 31, 2022, and Sept. 3, 2022, an unauthorized actor accessed and acquired certain files maintained on our servers," states the required notice, which was filed with the state last week.

State records list the span of the breach as beginning on July 31 and

ending Sept. 3.

On Friday, the district said the original one-day attack scenario remains correct.

"The investigation revealed that the threat actor was engaged in reconnaissance on or about July 31, 2022," a district statement said. "The cyberattack began and ended on Sept. 3, 2022."

For cybersecurity experts, the disclosure in the notice letter was no surprise. They had predicted that an investigation would uncover that the intrusion into the system began earlier than what had been announced.

"Hackers are often inside networks for weeks or even months before they deploy the ransomware that encrypts the systems," said Brett Callow, threat analyst for the cybersecurity company Emsisoft. "This means there's a window of opportunity during which threats can be detected and neutralized before they become full-blown ransomware incidents."

"In simple terms, a whole bunch of things happen before systems get locked," he added. "The hacker needs to do recon, to get into the network, to ensure they can get back in, to gain access to other areas of the network, to exfiltrate data, etc., etc. All of these steps require them doing certain things—and those things can be detected if you're looking for them."

A newly released Emsisoft report indicates that the annual number of known cyberattacks on school systems in 2022 was about the same as in other recent years despite "executive orders, international summits, increased efforts to disrupt the ransomware ecosystem, and the creation by Congress of an interagency body, the Joint Ransomware Task Force, to unify and strengthen efforts."

But it is unclear if the attacks are causing increased harm, according to the report.

"A decrease in the level of disruption caused by attacks or in the amount paid in ransoms could be regarded as a win even if the number of incidents had increased," the report states, while noting that data to draw such a conclusion was largely unavailable.

The L.A. Unified data-breach notice contained unwelcome news for district contractors based on the ongoing investigation.

"On Jan. 9, 2023, we identified labor compliance documents, including certified payroll records, that contractors provided to L.A. Unified in connection with Facilities Services Division projects," the notice states. "Those files contained the names, addresses and Social Security numbers of contractor and subcontractor employees and other affiliated individuals."

Carvalho, who became superintendent nearly a year ago, said recently that the district was more vulnerable because of preventable lapses. These included failing to follow through with key recommendations of an internal cybersecurity audit that was prepared more than two years ago, he said.