Hackers release data after LA school district refuses to pay ransom

October 3 2022, by Howard Blume

Credit: Pixabay/CC0 Public Domain

Hackers released data from the Los Angeles school district on Saturday, a day after Superintendent Albert Carvalho said he would not negotiate with or pay a ransom to the criminal syndicate.

Some screenshots from the hack were reviewed by the Los Angeles Times and appear to show some Social Security numbers. But the full extent of the release remains unclear.

The release of data came two days earlier than the deadline set by the syndicate that calls itself Vice Society—and happened in apparent response to what it took as Carvalho's final answer regarding whether the district would pay the hackers to prevent the release of private information and also to receive decryption keys to unlock some district computer systems.

"What I can tell you is that the demand—any demand—would be absurd," Carvalho told the Times on Friday. "But this level of demand was, quite frankly, insulting. And we're not about to enter into negotiations with that type of entity."

In a statement released later that day, he added: "Paying ransom never guarantees the full recovery of data, and Los Angeles Unified believes public dollars are better spent on our students rather than capitulating to a nefarious and illicit crime syndicate."

The extent of the data theft is now being evaluated by federal and local authorities.

Carvalho said on Friday that he believed confidential information of employees was not stolen. He was less certain about information related to students, which could include names, grades, course schedules, disciplinary records and disability status.

Whatever the case, he said, the district will provide assistance to anyone who is potentially harmed by the release of data, including by setting up an "incident response" line at (855) 926-1129. Its hours of operation are 6 a.m. to 3:30 p.m., Monday through Friday, excluding major U.S.

holidays.

Since the attack, which was discovered on Sept. 3, the nation's second-largest school district has worked closely with local law enforcement, the FBI and the federal Cybersecurity and Infrastructure Security Agency or CISA.

CISA posted a warning to education institutions about Vice Society immediately after the LAUSD attack without directly confirming that the syndicate was responsible for it.

The syndicate's original Monday deadline was posted on the dark web site maintained by Vice Society, which had informally confirmed to at least three reporters that it was responsible for the hack.

On Friday, Carvalho did not contest media accounts identifying Vice Society. He continued his previous practice of not naming the amount that is being demanded.

The claim of responsibility became official with a posting on the dark web. A screenshot shows the Vice Society logo and its catchphrase "ransomware with love." The site lists as "partners" the entities that it claims to have victimized. These now include the L.A. Unified School District, which is listed along with the district logo.

"The papers will be published by London time on Oct. 4, 2022, at 12 a.m.," the webpage stated. That deadline would fall eight hours earlier in Los Angeles when adjusted for the time change. A countdown clock ticked down the time.

Hackers this year have attacked at least 27 U.S. school districts and 28 colleges, according to cybersecurity expert Brett Callow, threat analyst for the digital security firm Emsisoft. At least 36 of those organizations

had data stolen and released online, and at least two districts and one college paid the attackers, Callow said.

Callow was among the cybersecurity bloggers and professionals who confirmed Sunday morning that the data had been posted.

Vice Society alone has hit at least nine school districts and colleges or universities so far this year, per Callow's tally.

When the attack was discovered, district technicians quickly shut down all computer operations to limit the damage, and officials were able to open campuses as scheduled on the Tuesday after the holiday weekend. The shutdown and the hack combined to result in a week of significant disruptions as more than 600,000 users had to reset passwords and systems were gradually screened for breaches and restored.

During this rebooting, technicians found so-called tripwires left behind that could have resulted in more structural damage or the further theft of data. The restoration of district systems is ongoing, but there also was another element of the attack: the exfiltration of data.

The hackers claimed to have stolen 500 gigs of data.

The district also has set up a cybersecurity task force, and the school board has granted Carvalho emergency powers to take any related step he feels is necessary.

The internal systems most damaged were in the facilities division. Carvalho said it was necessary to create workarounds so that contractors could continue to be paid and repairs and construction could continue on schedule.