University of California victim of nationwide hack attack

April 3 2021, by Robert Jablon

Credit: Pixabay/CC0 Public Domain

The University of California is warning its students and staff that a ransomware group might have stolen and published their personal data and that of hundreds of other schools, government agencies and companies nationwide.

A cybersecurity attack targeted a vulnerability in Accellion, a third-party vendor that is used to securely transfer files, the university said in a statement Wednesday.

"We understand those behind this attack have published online screenshots of personal information, and we will notify members of the UC community if we believe their data was leaked in this manner," the university said.

The hacker or hackers also have been sending threatening mass emails threatening to publish data "in an attempt to scare people into giving them money," the statement said.

In an update Friday, the university system said the cyberattack affected about 300 organizations, "including universities, government institutions and private companies."

Other schools, including Stanford University's School of Medicine and Yeshiva University in New York City, have reported that student and employee Social Security numbers and financial information were stolen and that some were posted online.

The information was obtained in December and January when hackers exploited a vulnerability in a 20-year-old Accellion file transfer service, various reports have said. However, some organizations said they only recently became aware of the breach.

The Baltimore Sun on Thursday reported that private information of staff members and students at the University of Maryland, Baltimore was posted online this week. The school said a hacking group known as Clop gained access to Accellion in December, the Sun said.

The University of Colorado and the University of Miami reported that

files were accessed in January and included personal data and some health, study and research data.

The Washington State Auditor's Office reported last month that information on nearly 1.5 million unemployment applicants had been stolen.

Accellion released a statement in March that said it had closed "all known" vulnerabilities and no new ones had been found.

Ransomware attacks on a massive scale and seeking massive payouts have hit several organizations in recent months.

In an unrelated attack, the computer system of one of the nation's largest school districts was hacked by a criminal gang that encrypted district data and demanded $40 million in ransom or it would erase the files and post students' and employees' personal information online. Broward County Public Schools, based in Fort Lauderdale, said in a statement Thursday that there is no indication that any personal information has been stolen and that it made no extortion payment to the ransomware gang.

An epidemic of ransomware attacks has been plaguing government agencies, businesses and individuals for the past three years. Most are Russian-speaking gangs based in Eastern Europe and enjoy safe harbor from tolerant governments. The more sophisticated groups identify their targets in advance, infect networks through phishing or other means and often steal data as they plant malware that encrypts a victim's network.

After the ransomware is activated, the criminals demand money to unlock the malware and refrain from posting—or selling—stolen data. In the case of corporations, that data could be trade secrets. In the case of retailers or government agencies it could be Social Security, bank

account numbers and birth dates.

Public school districts have been frequent targets of ransomware attacks. Overall, ransomware attacks disrupted learning at 1,681 schools, colleges, and universities in 2020 and at least 544 so far this year, said analyst Brett Callow at Emsisoft, a cybersecurity firm. Seven districts had personal data published.

The average ransom paid for to hacking gangs nearly tripled from $115,000 in 2019 to $312,000 in 2020, according to the cybersecurity firm Palo Alto Networks. It said the highest ransom paid by an organization doubled last year from to $10 million, up from $5 million in 2019.