UCLA confirms it was hit by cyberattack but offers few details

July 3 2023, by Nathan Solis

Credit: Pixabay/CC0 Public Domain

UCLA says it is the latest victim of a cyberattack, but university officials did not specify what information was accessed or whether any information was posted online.

The incident marks the latest attack that has claimed as victims hundreds of organizations and businesses including the U.S. Department of Health

and Human Services; the multinational law firm Kirkland & Ellis; the states of Oregon, Missouri and Illinois; the California Public Employees' Retirement System; the New York City Department of Education; the French multinational company Schneider Electric; and the Nova Scotia government, according to a list posted online by the ransomware group.

UCLA learned about a breach on May 28 in the system that the university uses to transfer files across the campus and to other entities, according to UCLA officials. The university implemented its incident-response procedure and patched the loophole used by the hackers with an update from Progress Software, the makers of a file transfer software product called MOVEit.

"The university notified the FBI and worked with external cybersecurity experts to investigate the matter and determine what happened, what data was impacted and to whom the data belongs. Those who have been impacted have been notified," a UCLA spokesperson said. "This is not a ransomware incident. There is no evidence of any impact to any other campus systems."

UCLA declined to provide more information about the attack or the suspected culprits, but information from roughly 16 million users has been stolen by the CL0P Ransomware Gang, according to technology experts tracking the cyberattack.

The group has exploited a vulnerability with the MOVEit Transfer tool, according to the Cybersecurity and Infrastructure Security Agency (CISA) with the Department of Homeland Security.

CL0P, also known as TA505, has taken data with a malware that gives the group access to user databases. Progress Software has been working with the Department of Homeland Security and the FBI to address the attacks, said Eric Goldstein, executive director for CISA.

"CISA continues to work diligently to notify vulnerable organizations, urge swift remediation, and offer technical support where applicable," Goldstein said.

Threat analyst Brett Callow with cybersecurity company Emsisoft said there are 148 known victims caught in the CL0P cyberattacks, with 11 organizations that have disclosed how many people were impacted by the breach. Callow wrote in a Twitter post that the data of 16.2 million individuals have been compromised.

"That number will increase significantly if/when the other 137-plus victims make a disclosure," Callow said.

In April 2021, UCLA was the victim of a cyberattack that resulted in a demand for a ransom and some personal information being published online. Other schools, including Stanford University's School of Medicine and Yeshiva University in New York City, reported that student and employee Social Security numbers and financial information were stolen and some were posted online during that attack.

2023 Los Angeles Times.

Distributed by Tribune Content Agency, LLC.