Netwalker ransomware continues assault on US colleges, hits UCSF

By Lawrence Abrams

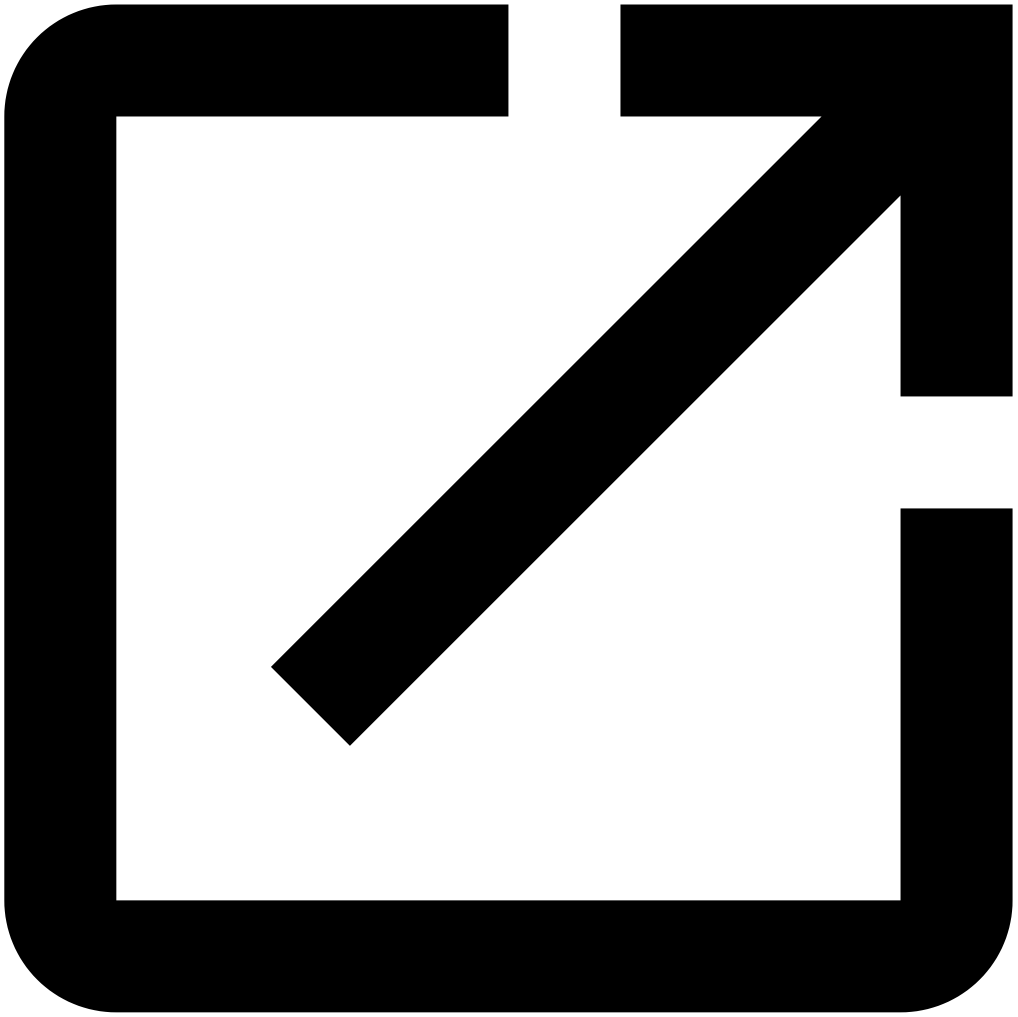
Published: 2020-06-03 · Archived: 2026-04-05 12:55:02 UTC

The Netwalker Ransomware operators claim to have successfully attacked the University of California San Francisco (UCSF), stolen unencrypted data, and encrypted their computers.

UCSF is a research university located in San Francisco, California, and is entirely focused on health sciences. According to the U.S. News & World Report's college rankings, UCSF ranks #2 in medical schools for research and #6 in best medical schools for primary care.

Over the past week, the Netwalker Ransomware operation has been targeting U.S. colleges and threatening to release their data

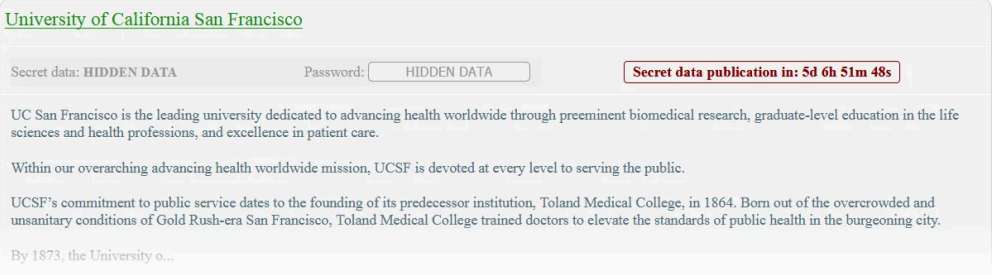

DIE LINKE.
0:00



On May 28th, Netwalker posted on their data leak that they had encrypted Michigan State University, and if a ransom was not paid, they would publicly release stolen data if not paid. This deadline has come and gone, and the ransomware operators have publicly released their data.

Next, they claimed to have attacked Columbia College of Chicago, and once again threatened to release the stolen data if not paid.

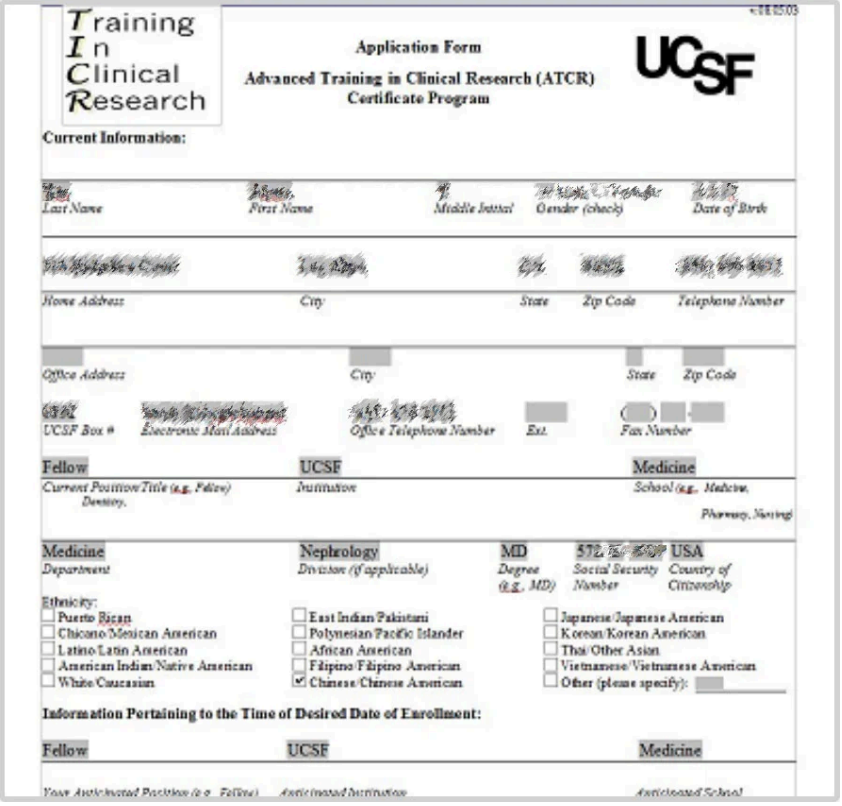
Today, Netwalker states that they allegedly attacked another U.S.-based college, University of California San Francisco.



UCSF entry on Netwalker's data leak site

As part of this leak, the threat actors have posted screenshots of some of the stolen files.

These images include student applications with social security numbers, a spreadsheet, and folder listings that appear to contain employee information, medical studies, and financials.



Leaked student application with SSN

BleepingComputer has contacted the University of California San Francisco to confirm the attack but has not received a reply.

Netwalker is becoming a bigger threat

Starting as the Mailto ransomware in October 2019, the ransomware rebranded as Netwalker in February 2020.

Netwalker has steadily been making a name for itself as it continues to announce a steady stream of successful attacks, including one against the Australian transportation company Toll Group,

This ransomware operation is known to target exposed Remote Desktop Services and use spam to gain access to enterprise-networks where it then steals unencrypted files before encrypting the computers.

As their latest disclosed victims have all been colleges, it may indicate a vulnerability in a commonly used application or device, or simply exposed Remote Desktop servers.

Source: https://www.bleepingcomputer.com/news/security/netwalker-ransomware-continues-assault-on-us-colleges-hits-ucsf/