Ransomware group targets universities in Maryland, California in new data leaks

By Written by

Archived: 2026-04-05 17:59:04 UTC

The Clop ransomware group has posted financial documents and passport information allegedly belonging to the University of Maryland and the University of California online.

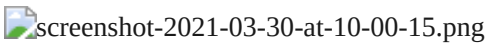
Security

On March 29, the threat actors began publishing screenshots of data allegedly stolen from the US educational institutes.

These screenshots, including records that allegedly belong to the University of Maryland, Baltimore, show a federal tax document, requests for tuition remission paperwork, an application for the Board of Nursing, passports, and tax summary documents.

The leaked data snapshots exposed sensitive information points including the photos and names of individuals, home addresses, Social Security numbers, immigration status, dates of birth, and passport numbers.

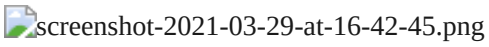
Sensitive information has been redacted in the screenshots below.



The University of California, Merced, also appears to have been subject to the same group's tactics.

Screenshots published by the group, viewed by ZDNet via Kela's threat intelligence suite Darkbeast, include lists of individuals and their Social Security numbers, retirement documentation, and 2019/2020 benefit adjustment requests.

In addition, the leaked data appears to include late enrollment benefit application forms for employees and UCPath Blue Shield health savings plan enrollment requests.



Clop has been linked to a string of cyberattacks against businesses. Clop is one of many threat groups that will employ a 'double-extortion' tactic, in which ransomware may be deployed on a compromised machine first, and then the cybercriminals threaten to make corporate or sensitive stolen datasets public on a leak site unless blackmail demands are met.

Earlier this month, the group leaked data allegedly belonging to the universities of Miami and Colorado.

On the same day, records allegedly belonging to Shell were also posted online. The oil giant revealed that a cyberattack had occurred through the compromise of Accellion FTA servers earlier this month.

On March 22, the REvil ransomware group published what appears to be financial data from tech giant Acer following a ransomware incident. Acer was subject to a $50 million ransom demand, of which it is not known if anything was paid. The company did not confirm that a ransomware attack occurred but did say that IT "abnormalities" had been discovered.

Update 14.20 BST: The University of Maryland, College Park, said the leaked sample files shared appear to relate to the Baltimore campus, UMB, rather than UMD, as listed.

Update 1.4.21 / 14.21 BST: A UMB spokesperson told ZDNet:

> "In late December, a criminal ransomware organization known as Clop breached the security of our Accellion file transfer system. This system was used by our students, faculty, and staff to transfer encrypted files. We discovered the breach earlier this week, when the hackers posted evidence that they had accessed a limited number of files in our system containing some personally identifiable information.
>
> There is no evidence that the file transfer system was compromised at any other time up to the date it was decommissioned and replaced in February.
>
> The university has reached out to the owners of the compromised files and offered them security assistance, including free credit monitoring and identity restoration services. We have also informed federal and state authorities of this incident.
>
> Every appropriate security measure was taken by our Center for Information Technology Services, including rigorous monitoring and the timely installation of all patches and upgrades provided by Accellion."

Previous and related coverage

- FBI warns of rise in PYSA ransomware operators targeting US, UK schools
- Ransomware gangs have found another set of new targets: Schools and universities
- 2020 was a 'record-breaking' year in US school hacks, security failures

---

Have a tip? Get in touch securely via WhatsApp | Signal at +447713 025 499, or over at Keybase: charlie0
