Ransomware gang leaks data stolen from Colorado, Miami universities

By Lawrence Abrams

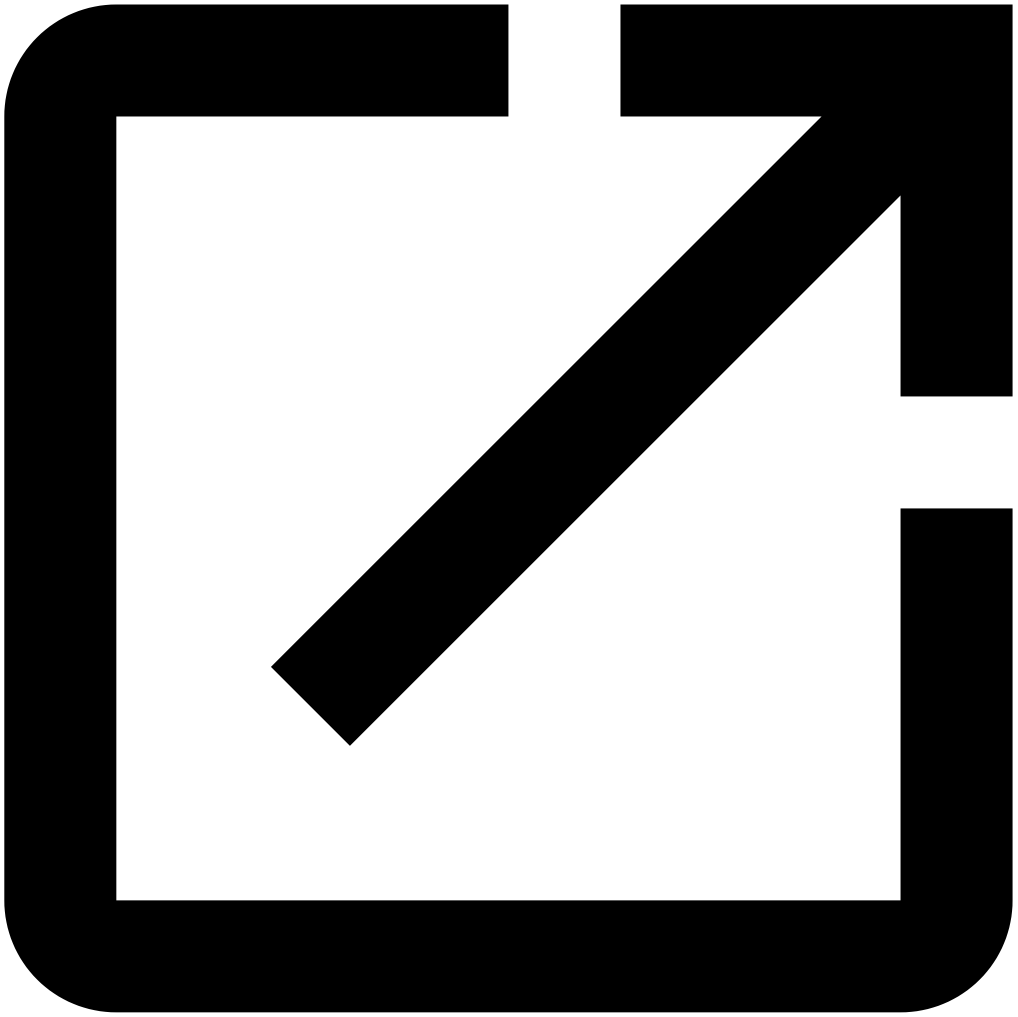
Published: 2021-03-23 · Archived: 2026-04-05 14:31:10 UTC

Grades and social security numbers for students at the University of Colorado and University of Miami patient data have been posted online by the Clop ransomware group.

Starting in December, threat actors affiliated with the Clop ransomware operation began targeting Accellion FTA servers and stealing the data stored on them. Companies use these servers to share sensitive files and information with people outside of their organization.

The ransomware gang then contacted the organizations and demanded $10 million in bitcoin or they would publish the stolen data.


DIE LINKE.
0:00



> Hello!
>
> Your network has been hacked, a lot of valuable data stolen. <description of stolen data, including the total size of the compressed files> We are the CLOP ransomware team, you can google news and articles about us. We have a website where we publish news and stolen files from companies that have refused to cooperate. Here is his address http://[redacted].onion/ - use TOR browser or http://[redacted].onion.dog/ - mirror. We are visited by 20-30 thousand journalists, IT experts, hackers and competitors every day. We suggest that you contact us via chat within 24 hours to discuss the current situation. <victim-specific negotiation URL> - use TOR browser We don't want to hurt, our goal is money. We are also ready to provide any evidence of the presence of files with us.

Ransom note sent to Clop victims

Since February, the Clop ransomware operation has been publishing files stolen using vulnerabilities in Accellion FTA file-sharing servers.

Clop is now publishing student, university data

This week, the Clop ransomware gang started publishing screenshots of files stolen from Accellion FTA servers used by the University of Miami and Colorado.

In February, the University of Colorado (CU) disclosed that they suffered a cyberattack where threat actors stole data via the Accellion FTA vulnerability.

"While the full scope has not yet been determined, early information from the forensic investigation confirms that the vulnerability was exploited and multiple data types may have been accessed, including CU Boulder and CU Denver student personally identifiable information, prospective student personally identifiable information, employee personally identifiable information, limited health and clinical data, and study and research data," CU's data breach notification stated.

The Clop ransomware has begun to post screenshots of the stolen data, including university financial documents, student grades, academic records, enrollment information, and student biographical information.

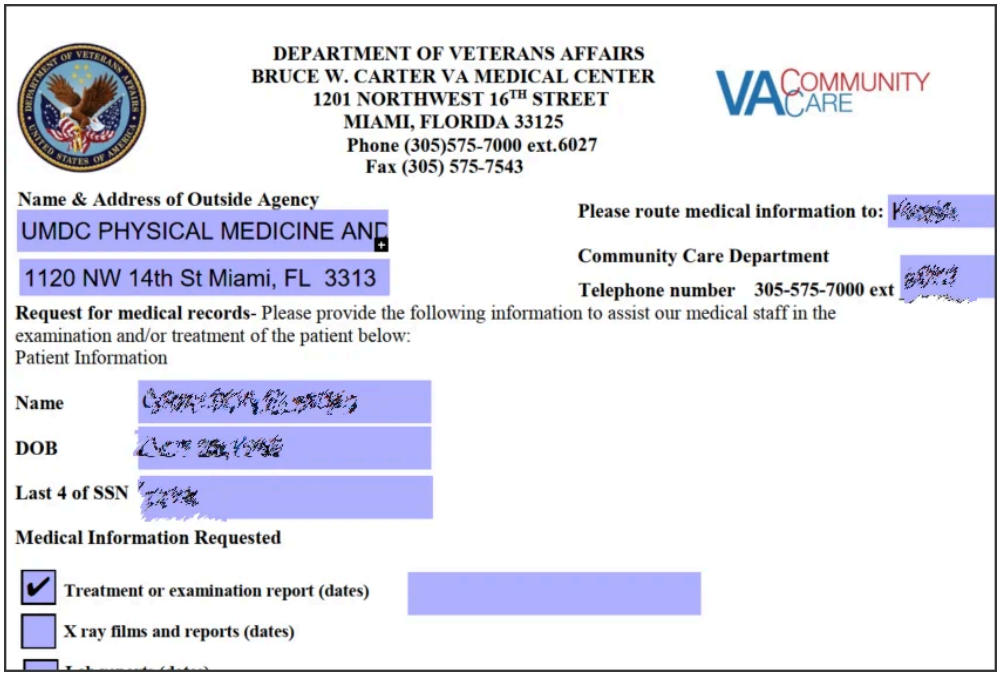
While the University of Miami did not disclose a data breach, they did use a secure file sharing service called 'SecureSend' that has since been shut down.

"Please be advised that the secure email application SecureSend (secure.send.miami.edu) is currently unavailable, and data shared using SecureSend is not accessible," reads the University's SecureSend page.

From URLs found by BleepingComputer, this SecureSend service was also powered by an Accellion FTA server.

While the University of Miami never disclosed a security incident, the Clop ransomware operation also published screenshots of patient data.

This data includes medical records, demographic reports, and a spreadsheet with email addresses and phone numbers.



DEPARTMENT OF VETERANS AFFAIRS
BRUCE W. CARTER VA MEDICAL CENTER
1201 NORTHWEST 16TH STREET
MIAMI, FLORIDA 33125
Phone (305)575-7000 ext.6027
Fax (305) 575-7543

VA COMMUNITY CARE

Name & Address of Outside Agency
UMDC PHYSICAL MEDICINE AND
1120 NW 14th St Miami, FL 3313

Please route medical information to: [redacted]
Community Care Department
Telephone number 305-575-7000 ext [redacted]

Request for medical records- Please provide the following information to assist our medical staff in the examination and/or treatment of the patient below:
Patient Information

Name [redacted]
DOB [redacted]
Last 4 of SSN [redacted]

Medical Information Requested

☑ Treatment or examination report (dates)
☐ X ray films and reports (dates)

Medical records leaked by Clop

The data allegedly stolen from the University of Miami appears to belong to patients of the University's health system.

The University of Miami shared the following statement, which can be read in full below.

> "The University of Miami is currently investigating a data security incident involving Accellion, a third-party provider of hosted file transfer services. We take data security seriously and data protection is a top priority. As soon as we became aware of the incident, we took immediate action to investigate and contain it. We also retained leading cybersecurity experts to assist with our investigation. We have reported the incident to law enforcement and are cooperating with their investigation. Based on our investigation to date, the incident was limited to the Accellion server used for secure file transfers and did not compromise other University of Miami systems or affect outside systems linked to the University of Miami's network."
>
> "While we believe based on our investigation to date that the incident is limited to the Accellion server used for secure file transfers, we continue to enhance our cybersecurity program to further safeguard our systems from cyber threats. We continue to serve our University community consistent with our commitment to education, research, innovation, and service." - University of Miami.

At this time, the ransomware gang has only released a few screenshots for each University but will likely release more files in the future to pressure the victims to pay.

Other Accellion FTA victims extorted by Clop include the supermarket giant Kroger, the Reserve Bank of New Zealand, the Australian Securities and Investments Commission (ASIC), Singtel, QIMR Berghofer Medical Research Institute, and the Office of the Washington State Auditor ("SAO")., and the energy company Shell,

Update 3/23/21 08:24 PM EST: Added statement from University of Miami.
