SECURITY

Clop ransomware gang breaches University of Colorado and University of Miami

March 25, 2021

Clop ransomware group has allegedly hacked the grades and social security numbers for students at the University of Colorado and patient data of the University of Miami.

According to BleepingComputer, cybercriminals with the Clop ransomware group have been targeting Accellion FTA servers and stealing sensitive data. Accellion is a third-party provider of hosted file transfer services. The group has contacted organizations and demanded $10 million in bitcoin with the threat of publishing the data if payment was not received.

Now, the group has started to leak student and university data stolen from the University of Miami and Colorado. In a data breach notification, the University of Colorado said, "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."

The University of Miami later said they were investigating a data security incident involving Accellion. "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," the University of Miami said.

Joseph Neumann, Cyber Executive Advisor at Coalfire, a Westminster, Colorado-based provider of cybersecurity advisory services, says, “Universities have always been a soft target for any type of cyber attacks. Due to their commitment to openness, learning institution’s security is commonly a backseat to allowing the free movement of thoughts and ideas. Ransomware attacks are not only

plaguing educational institutions but everyone equally, due to the ability of attackers to quickly monetize access and data they are able to get ahold of. These specific attacks are a little unique with the exfiltration of data vs just encrypting the data that is shown in a vast majority of ransomware attacks."

Timur Kovalev, chief technology officer at Untangle, a San Jose, Calif.-based provider of comprehensive network security for SMBs, says, "Ransomware cyberattacks exploded in 2020, taking advantage of the unique circumstances brought on by the pandemic. These attacks quickly became top of mind for businesses. In fact, in Untangle's 2020 SMB IT Security Report, 75% of respondents said that recent security breaches and ransomware attacks in some way affect the way they view their security roadmap."

Kovalev adds, "In 2020, Criminals particularly took aim at educational institutions with the rapid shift to online learning and university employees working from home. The University of Utah was the victim of a ransomware attack and paid over $450,000 to prevent information from being released on the dark web. Taking another approach was Michigan State University who, despite threats to release student records and financial documents, refused to pay the ransom. While it may make sense to pay ransom in some events, it can set a bad precedent and encourage further attacks.

"This year, as we've seen with the attacks of the University of Colorado and University of Miami, the attacks are not only continuing, but becoming more sophisticated. To protect their data, students and employees at universities need to take the following steps," says Kovalev:

- It's important to block the ransomware using technology such as a Next Generation Firewall, which scans all network traffic for ransomware, and blocks it before it can get a hold on devices.
- It's imperative to continually train and remind employees of the correct actions to take to avoid activating ransomware attacks. In the Untangle survey, 24% of respondents cited employees who don't follow the guidelines as a barrier to IT security.
- Ensure your network is designed to isolate and minimize a ransomware attack. Segregate networks by setting up separate networks for different types of usage and/or roles. For example, have a guest network that is completely separate to the main network.
- Always have up to date backups. If your data is backed up, even if ransomware cripples the network or requires a complete reinstall on devices, a backup can revert the machine to the data it had on it the day before the attack, minimizing losses."