


Jeffco Public Schools hit by the same threat actors that hit Clark County School District — and via the same way

 databreaches.net/jeffco-public-schools-hit-by-the-same-threat-actors-that-hit-clark-county-school-district-and-via-the-same-way/

Dissent

November 2, 2023

How many school districts have to get massively hacked by the same method before the U.S. Department of Education, CISA, and states start really pressuring public school districts to address well-known vulnerabilities that are being exploited? Maybe that shouldn't be a rhetorical question.

Last night, DataBreaches was contacted by the same threat actors who claimed responsibility for the [hack and data leak](#) involving **Clark County School District** (CCSD) in Nevada. Of special note, in an interview with DataBreaches, they revealed [how they had gained access](#) to the district's network.

SingularityMD (as the threat actors call themselves, but note there is no connection to a business with the same name) provided DataBreaches with a link to a notice by **Jeffco Public Schools in Colorado**. The [notice](#), dated November 1, stated:

On October 31, some Jeffco staff members received alarming email messages from an external cybersecurity threat actor – an individual who has allegedly committed an illegal cybercrime against an institution or organization – indicating a cyber-attack. Jeffco's Information Technology team is working together with cybersecurity experts and law enforcement to determine the credibility of the attack and scope of the incident. This is a cyberthreat and there is no concern related to physical safety.

Jeffco Public Schools takes data security very seriously and has procedures in place to respond to this type of situation given the unfortunate frequency of such incidents across all industries including education. Keeping our students and staff safe and communicating openly with our families are core to Jeffco's values.

This webpage will be updated with more information as it becomes available.

There has been no substantive update since then.

The “alarming message”

The “alarming message” was an email with the subject line **Notice of Security Breach**.

The sender was “Anihi Blep” using a mail.com address. DataBreaches had received email from that sender and email address in the past following the CCSD breach. The body of the email began:

We, SingularityMD have included a few relevant parties directly and a selection of principals on cc.

Your overall approach to cyber security is too relaxed.

We have illegally accessed your network and downloaded the following:

- Staff phone, home addresses, title and a few other details.
- Parent and Student contact information (past and present) – 90,000 students
- Student school email addresses, emergency contacts name, phone and email, student birthdates – 90,000 students
- Full backup of your IT project management directory (this includes past and present projects, lots of confidential information and system configurations)
- Accessed the Follet FTPS from the project management directory and downloaded a full student list (outdated). We already have this through your other systems such as infinite campus.
- Some financial documents
- Extracts from Group conversations (Golden HS Staff and Admin > 2000 conversations and files)
- Full extract of IEP's (Individualized Education Program) as at 2020

The message pointed recipients to previous reporting by DataBreaches about the CCSD breach and then noted:

Either you can pay a fee for disposal of the stolen information or it will be uploaded and made broadly available.

This cyber breach has not been politically motivated in any way, and is viewed by us as a business transaction. We are the same team as behind Clark County School District on the 5th October. They chose not to pay, we are eager for an opportunity to prove that we will destroy the documents on payment as you will not be the last organization we work with. Due to the above factors the fee for disposal in this instance, has been reduced to be far below what it should be.

The fee was listed as \$15,000 in monero, to be paid by November 7.

Links to proof of claims were provided and the email also spelled out the consequences for failure to pay:

1. All information will be uploaded to the dark web, and to the internet (repeatedly) in an easily digestible format
2. Included information about poor security practices on your part will be specifically mentioned in a top-level readme file

3. Using all the Contact information available from your network, every affected parent and staff member will be emailed with this information and links to this data leak with suggestions of a class action.
4. News and media will be informed.

A copy of the email, redacted by DataBreaches, appears below this article.

Second Verse, Same as the First

DataBreaches contacted SingularityMD to ask them some preliminary questions. In response, they noted that the first gained access to Jeffco about six months ago — *using exactly the same methods that they reported using for CCSD*. Once again, a district's policy of using students' date of birth as their password enabled threat actors to relatively easily gain access to the network. In discussing **the CCSD attack** with DataBreaches, SingularityMD (SM) had stated:

SM: We compromised a student account, then accessed information available to any student to escalate from there to teacher to systems level access for one or two systems. This was not a fancy high tech operation.

When DataBreaches asked how they were able to access the student's account, they responded that they obtained the student's date of birth (YYYYMMDD) from social media, and the email address from the student's account on "TikTok, etc." where the student ID had been used as the username because the student authenticated their school account when setting up the social media account. Asked to explain what information was available to any student that allowed them to escalate from the student's account to teacher to systems level, they replied:

SM: Google groups and google drives, if not configured correctly will expose teachers and staff files and conversations. In rare instances teachers have created shared drives and given the google group access to this drive. So if one was to add themselves to the group, they can then also access the drive contents. Nothing fancy at all.

According to SingularityMD, Jeffco's security was not as weak as CCSD's: "They are better than CCSD. Though their IT Project Management Office have made some significant blunders placing backups and system configuration files in arm's reach by virtue of the same methods as used in CCSD – public groups and share drives. Nothing Fancy." But they added:

They are blocking student accounts I message them from, but do not realize that we can literally log into 1 in 4 student accounts so have an endless supply of 80k accounts. So this would be points taken off.

DataBreaches will be following up on this incident and notes that Jeffco did not respond to an email inquiry sent to it last night asking it to confirm or deny whether it used date of birth as student passwords and whether the district was requiring an immediate password reset that doesn't involve the use of date of birth.

The risks of using date of birth as passwords for student accounts has been recognized for years. The CCSD breach has affected more than 200,000 students. The Jeffco one allegedly affects 90,000 students. Both breaches also affect district employees.

So when will the U.S. Department of Education and/or states make it absolutely clear that districts should not use date of birth as passwords and that districts may risk state enforcement action and/or risk losing federal funding for failure to adequately protect student information if they continue to do so?

JeffcoEmail