

# Back to School: Why Cybercriminals Continue to Target the Education Sector | Part Two

---

 [ke-la.com/back-to-school-why-cybercriminals-continue-to-target-the-education-sector-2/](https://ke-la.com/back-to-school-why-cybercriminals-continue-to-target-the-education-sector-2/)

September 14, 2020

## A New Year, a New Beginning, and a New Round of Cyber Threats

---

2020's back to school is a bit different than usual as most students around the world are getting ready to meet again with their peers online. Rather than worrying about the classic back to school activities, such as purchasing the most in-style school supplies or figuring out the perfect outfit for day 1, students are more invested in finding the comfortable home setup for online learning. School IT admins, on the other hand, are most concerned this year about educating their students and staff regarding cybersecurity as school begins remotely, while in parallel focusing heavily on deterring cyber threats from cybercriminals looking to attack educational institutions.

In our last blogpost, [Back to School: Why Cybercriminals Continue to Target the Education Sector, Part 1](#), we looked into threat actors' overall interest in targeting organizations in the education sector, diving into some examples of recent attempted attacks that we've spotted across the underground ecosystem. This blogpost touched on several key points that helped establish a general understanding of the threat level targeting educational institutions. We decided to circle back to this topic because of the increasing risks that emerged as much of the world begins to return to schools.

Schools already struggling with [high cases of COVID-19](#) now must begin battling other mishaps such as cyberattacks on their online learning platforms within their first days of remote learning. This situation occurred to one of the largest district schools in Florida and was likely caused by a newbie in the underground world – an alleged [16-year old threat actor](#). This successful attack on a large school, by a supposedly young threat actor, may imply that planned attacks by more sophisticated and experienced threat actors are similarly on their way.

## Summer's Over, but the Fun's Just Beginning (for Cybercriminals)

---

Since the release of our last post, we continued to monitor threat actors' interest in the education sector and laid out what other threats were seen in the underground ecosystem.

Over the last month, KELA closely monitored many underground communities as well as specialized auto shops where underground actors buy and sell credentials enabling [remote access to compromised websites and services](#). Out of more than 45 remote accesses that we tracked over August alone, across the most popular three underground forums, we

noticed that 7 of those belong to educational institutions. These accesses were being sold mainly to UK or US educational institutions – with a couple in Australia and singles in Israel and Germany, too – at prices ranging from as little as 200 USD to as much as 17,000 USD.

Active Directory networks (Domain admin/Enterprise Admin access)

Aug 4, 2020

NO AVATAR

Aug 4, 2020

**University located in Florida, USA - domain admin/enterprise admin - 1.5 BTC**

London executing broker (brokerage services, foreign currency exchange) - domain admin - 0.5 BTC

Switzerland real estate network (publicly traded on Swiss exchange) - domain admin - 0.3 BTC

France health care organization - domain admin - 0.1 BTC

city in Sardinia, Italy - domain user 0.05 BTC

Mexico credit union network - domain user - 0.05 BTC

Israel supply chain network - domain user - 0.05 BTC

I accept guarantor for all sales, I also have deposit on exploit. check my profile

Report

Private School located in UK Enterprise/Domain Admin

Aug 22, 2020

NO AVATAR

Пользователь

Joined: Feb 10, 2019  
Messages: 17  
Reaction score: 0

Aug 22, 2020

Titlle say most,

Have access to the DC with Enterprise/Domain user right  
RDP access

Sophos Installed  
Veritas Backup Exec

\$5M revenue  
24 hots at the moment of the scan

I dont really have a price, make me a reasonable offer over pm

We tried to assess what the price differences could mean in terms of the victims being targeted. At times, it's difficult to understand how valuable an access may be, solely based on price and the limited detail published by the threat actor. However, after more in-depth review of the accesses, we noticed that much of the time, threat actors are pricing the goods as they would with any other business – based on the revenue of the victim at hand. The

educational institutions are viewed by many threat actors as just another business with growing revenue – and in that case, growing profits for the threat actors. Another factor that influences the price is access rights – whether the buyer will have access as a user or with administrator privileges.

The relatively high price and the speed at which some listings are purchased do indicate the high demand for these items in the underground ecosystem. For example, one of the listings was published for 5,660 USD and sold in less than a week.

Опубликовано: В пятницу в 09:51

байт

Hello guys, im new to this forum I came from [REDACTED]

Have at the moment 2 full access for sale

**Private School UK Full Domain Admin/Enterprise Admin**  
Access to the network around 17-20 pcs at the moment of the scan (including DC and Backups)  
Employees: 30  
Revenue: \$5 Million ([REDACTED])

5 публикаций  
Регистрация  
28.08.2020

**Price 0.05 BTC**

Though remote access has been growing in popularity in the underground ecosystem over the last few years, compromised data still holds a significant place for cybercriminals. For example, emails and passwords of a Singaporean school have been recently leaked for free, and personal data pertaining to US students has been offered for sale across underground marketplaces. **In addition, we've recently spotted credentials to 4 different university FTP servers, some of which contain internal data – also leaked for free.**

PLAINTEXT [REDACTED]

by [REDACTED] - August 31, 2020 at 06:37 PM

New Reply

August 31, 2020 at 06:37 PM #1

18037 mail:pass

**base**

https: [REDACTED]

New User

**MEMBER**

Posts 13  
Threads 6  
Joined Aug 2020  
Reputation 0


PM Find

Reply Quote Report

« Next Oldest | Next Newest »

Enter Keywords Search Thread

**SELLING** 【usa student】 9k line usa student full data  
 by [redacted] August 31, 2020 at 01:20 PM New Reply



New User

**MEMBER**

Posts 5

August 31, 2020 at 01:20 PM This post was last modified: August 31, 2020 at 01:23 PM by [redacted] #1

country: us  
 line: 9874  
 price: 100 usd  
 column:

Phone Email first\_name last\_name gender birthday location home\_town relationship\_status Education year Work


.....

a school shell, some student in usa. if u want buy some school web shell in usa , plz pm me thx

---

one hand data No bargaining

**FTP Servers of EDU Websites**  
 by [redacted] August 29, 2020 at 09:38 AM



New User

**MEMBER**

Posts 9  
 Threads 3  
 Joined Aug 2019  
 Reputation 0

1 YEAR OF SERVICE

August 29, 2020 at 09:38 AM

[redacted].edu/  
 [redacted].edu/  
 [redacted].edu/  
 [redacted].edu/

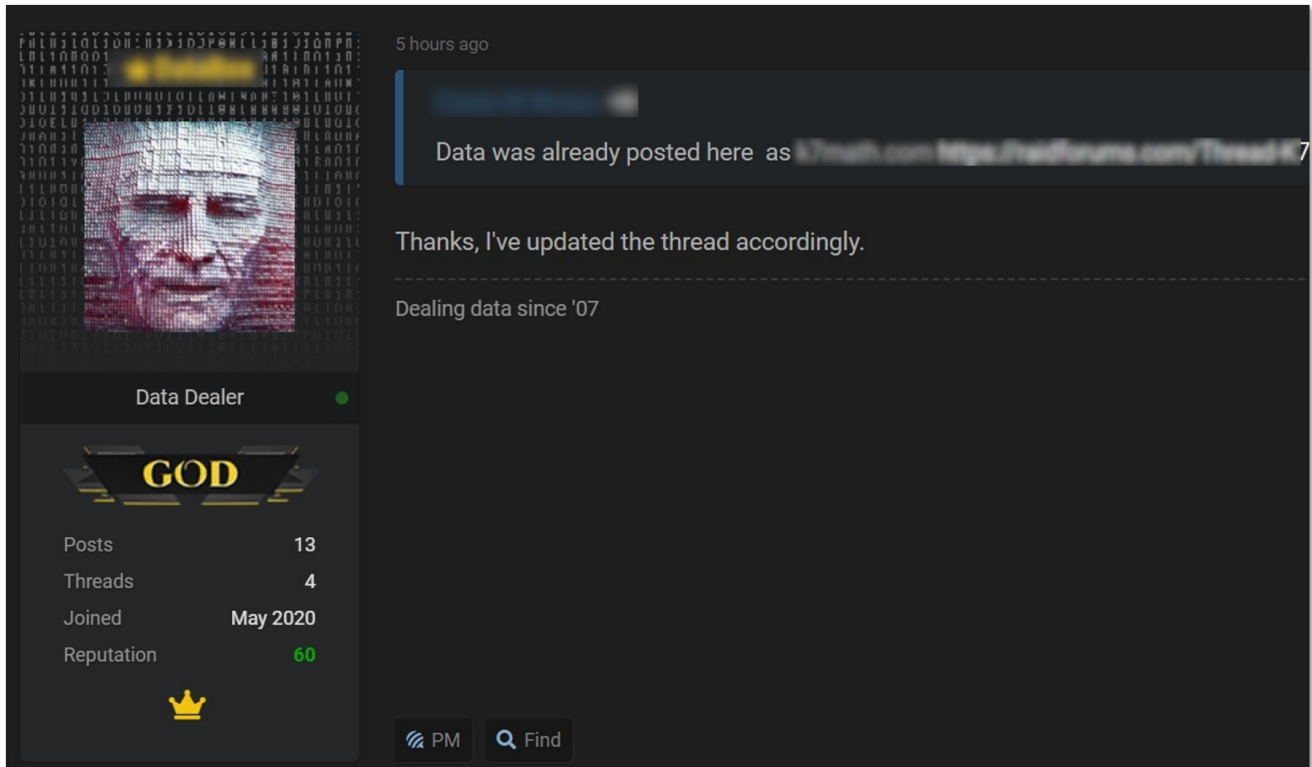
**Hidden Content**

---

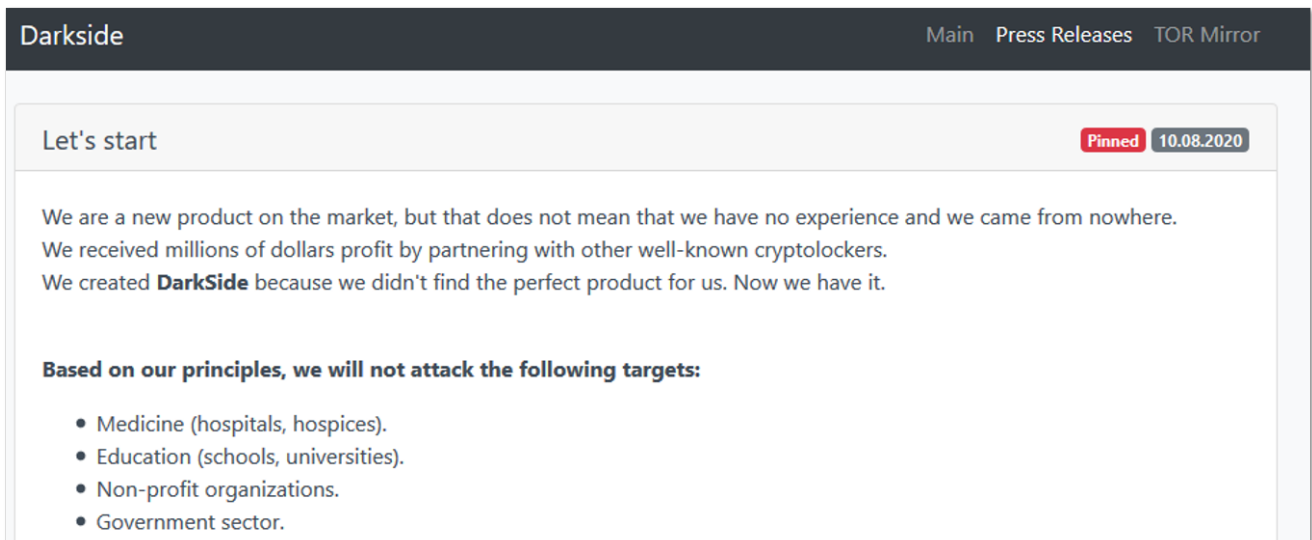
ftp://ftp.[redacted]  
 ftp://ftp.[redacted]  
 ftp://ftp.[redacted] Sometimes Accessible, Sometimes Unavailable]  
 ftp://ftp.[redacted]

PM Find

**Some underground threat actors have been seen leveraging previously sold/leaked data pertaining to educational institutions. In a recent post, a threat actor published that he was offering data pertaining to an Australian Education Department, where upon further research, it turned out to be K7math – an online service providing school e-learning solutions – which was previously leaked in March. In both of these instances – both the initial March listing, and the later one – the data was leaked for free, likely a stunt for the threat actors looking to gain some good reputation in the underground communities.**



As we continued to browse through different underground communities, we still noticed that there are newer players in the field who still claim against targeting the education sector. For example, DarkSide, the new ransomware gang that has recently emerged, states that it doesn't attack schools and universities. However, it's unlikely that most cybercriminals will adopt this attitude since they couldn't even get on board in terms of targeting medical institutions during a pandemic.



## Educational Institution Defenders: “Wake Me Up When September Ends”

Defenders of educational institutions are likely still adapting to this new norm, but it really comes down to two main actions that may help them deter attacks in the most efficient way possible.

1. **Educate** – The safety of these institutions is nothing less than team effort. These defenders must invest in standard cybersecurity awareness for all students and staff to ensure that best practices are held in order to keep personal information and information systems secure. The potential damage that can be caused may begin from a small mistake caused by one individual, for example opening a malicious attachment received via email, which may enable a threat actor the initial foothold required to enter the institution's systems.
2. **Invest in Threat Intelligence** – Cyberattacks generally occur after a long process of several different details combined. Organizations – and specifically in this case, educational ones – must invest in strategic monitoring of their assets, whether it be their domains, IT admins' personal details, IP addresses, or any other assets that can help threat actors initiate an attack on them. By investing in technologies that enable efficient and undetectable monitoring of their assets in underground marketplaces and forums, educational institution defenders can better prepare themselves for potential incoming threats that are targeting them.