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

ke-la.com/back-to-school-why-cybercriminals-continue-to-target-the-education-sector/

August 3, 2020

Just a few of the major headlines regarding the education sector have looked like this over the last couple of months:

Blackbaud Hack: Universities Lose Data to Ransomware Attack

The University of California Pays $1 Million Ransom Following Cyber Attack

University of York Discloses Data Breach, Staff and Student Records Stolen

The past year has seen a rise in the amount of education-related institutions that have been affected by cyberattacks. In 2019 alone, the K-12 cyber incident map reported that 348 schools have publicly-disclosed that they've been a victim of a cyberattack. That's just in the United States and doesn't even take into account the universities and colleges, which would by all means cause those numbers to escalate.

These statements got us wondering.

- Are underground threat actors actively looking for and interested in targeting organizations in the education sector?
- What types of attacks are we seeing affecting the education sector?
- What have been some of the recent attempted attacks that we've seen in the underground ecosystem?
- Are these targeted attacks on the universities themselves or are they stemming from access through a third-party provider?

These are all questions that will be addressed throughout this blogpost.

Cybercriminals Looking for the Big Money

At first glance, educational institutions, such as universities, local and state district schools, colleges, and others, may seem of little to no worth to underground threat actors. However, if that were the case, it would likely have nothing to do with the ethical factors of attacking educational institutions – something that *was* taken into consideration by threat actors discussing targeting the health sector.

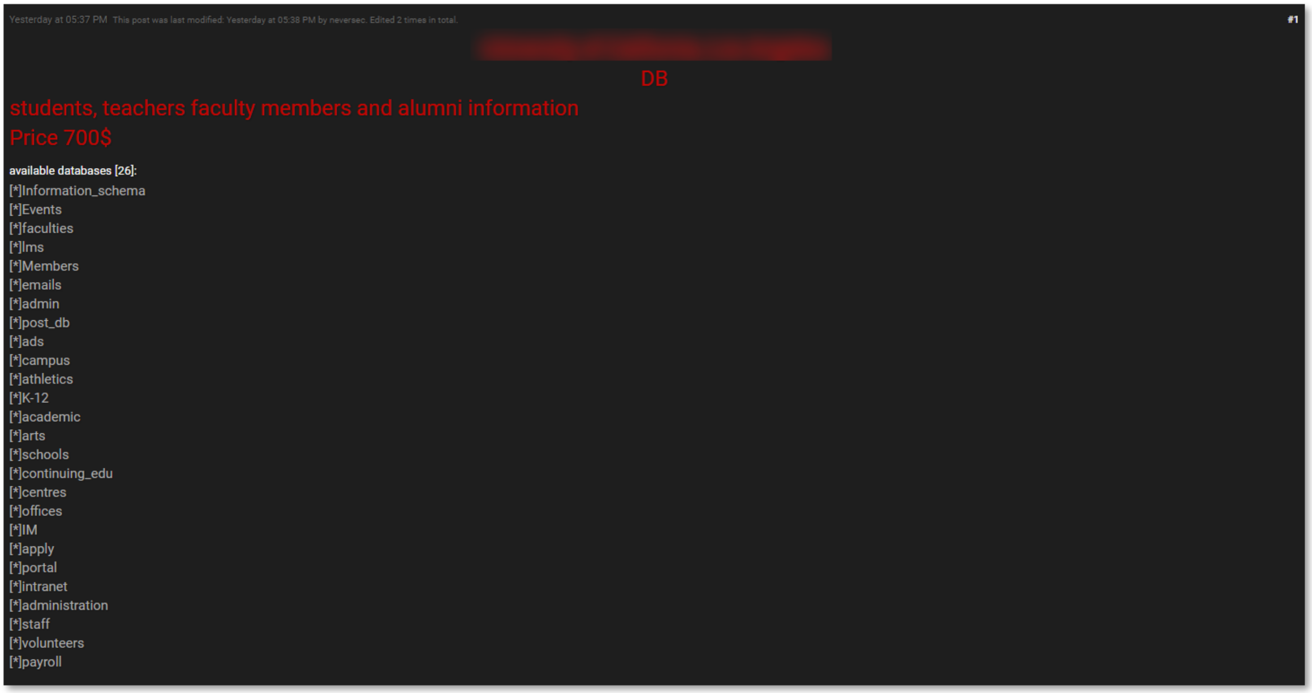
While browsing through various underground forums, we've found many threat actors claiming that they're not looking to target any businesses that have annual revenue less than $300 million, or any institutions in the government, education, healthcare, hotel and e-commerce sectors. What do (cybercriminals assume) those may have in common? It's merely a matter of profiting maximally. Underground cybercriminals don't seem to view the big money from attacking the organizations listed above, and therefore prefer to place their efforts elsewhere.

Though many cybercriminals seem to stand behind this, we still noticed that there are still a good amount of them that do in fact choose the route of targeting educational institutions as they do see potential profits, and sometimes even very big ones. The following section in this post will dive into how institutions in the education sector are being targeted in all different ways, causing some of them to eventually incur severe financial costs.

A Look into Educational Institution Attempts and Attacks

From large databases posted for sale, to remote admin access available on auto shops, and ransomware negotiations, institutions in the education sector have seen heaps of different threats and potential attacks.

Just last week, analysts at KELA noticed two university databases being sold on an underground forum – one pertaining to a London-based college, and the other to the university in California – both sold by the same actor, "Neversec."



Yesterday at 05:37 PM This post was last modified: Yesterday at 05:38 PM by neversec. Edited 2 times in total. #1

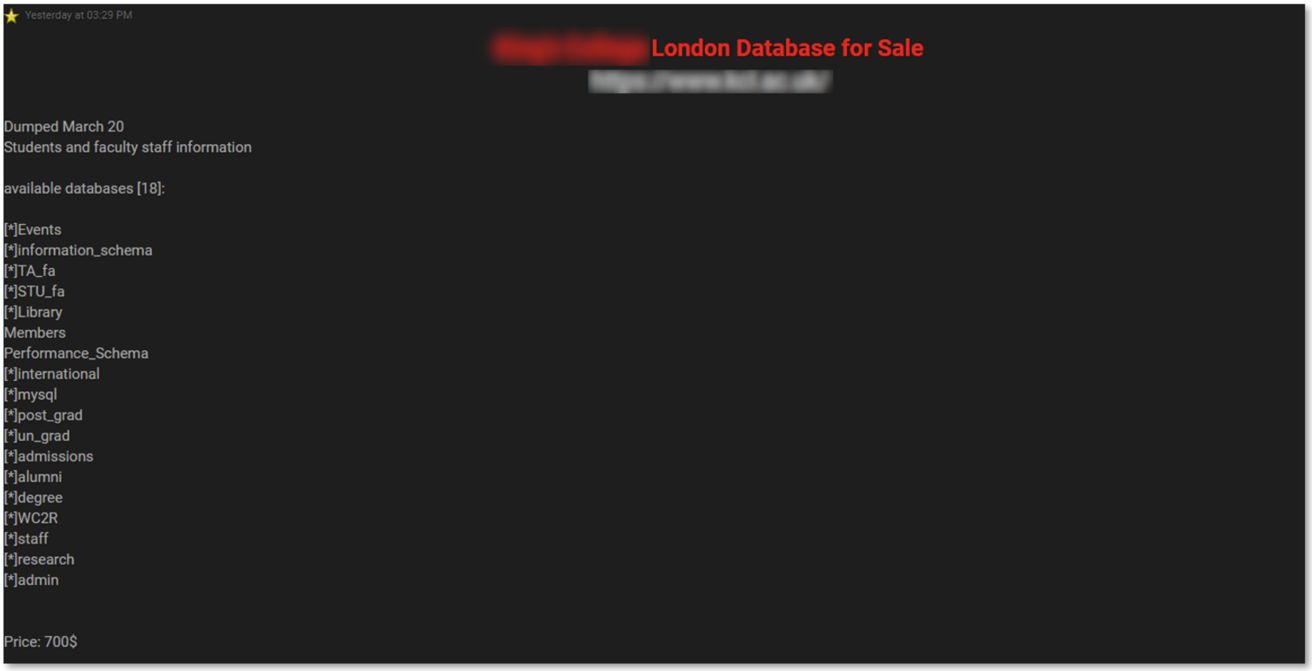
[redacted]

DB

students, teachers faculty members and alumni information

Price 700$

```
available databases [26]:
[*]Information_schema
[*]Events
[*]faculties
[*]lms
[*]Members
[*]emails
[*]admin
[*]post_db
[*]ads
[*]campus
[*]athletics
[*]K-12
[*]academic
[*]arts
[*]schools
[*]continuing_edu
[*]centres
[*]offices
[*]IM
[*]apply
[*]portal
[*]intranet
[*]administration
[*]staff
[*]volunteers
[*]payroll
```



★ Yesterday at 03:29 PM

[redacted] London Database for Sale

[redacted]

```
Dumped March 20
Students and faculty staff information

available databases [18]:

[*]Events
[*]information_schema
[*]TA_fa
[*]STU_fa
[*]Library
Members
Performance_Schema
[*]international
[*]mysql
[*]post_grad
[*]un_grad
[*]admissions
[*]alumni
[*]degree
[*]WC2R
[*]staff
[*]research
[*]admin


Price: 700$
```

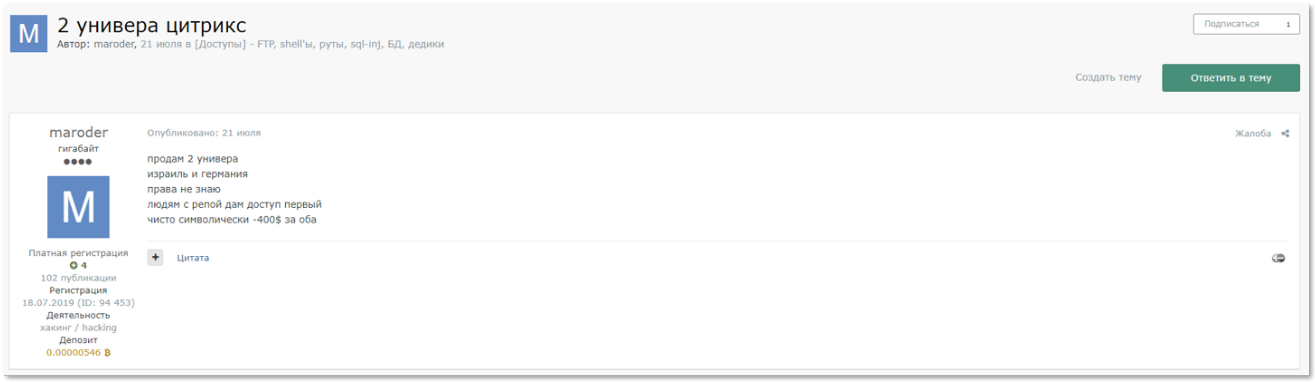
Following a quick assessment on this threat actor, our team assessed that Neversec is a rather new threat actor who registered on this forum on July 11. His past activities showed him selling databases belonging to a Saudi Arabian company and government agencies in the Dominican Republic, Chile, and Malaysia. Additionally, we found him sharing two guides for cybercriminals across underground forums, one of them being the StationX guide and cybersecurity course. In the case of the two institutions listed above, Neversec claimed that he successfully managed to obtain the databases directly from the institutions' systems themselves.

Once we acquired samples and began our analysis, we found that the two databases contain at least first and last names, emails, phone numbers, and addresses. Though small in quantity – 1,800 records for the California-based university and an even smaller 720 for London one – we weren't quick to deem this unimportant just yet. These credentials – belonging to the institutions' students, staff, and alumni – can be leveraged for phishing attacks, something that could provide threat actors with an initial foothold into the networks of the universities. Once they've got this first foot in the door, threat actors may easily use this unprivileged access to further explore the victims' networks and may eventually deploy ransomware or other malware on the institutions' systems.

Take the case of the University of California, for example. Though we do not know if it was as a result of a compromise through phishing emails, the university paid a ransom of more than $1 million. As with any business, cybercriminals must start from somewhere and all they need is that initial foothold – something that compromised credentials may assist them with.

Browsing further through some cybercrime forums, we stumbled upon a threat actor going by the handle “maroder” (previously “ailing”) posting access to two university networks for sale. In his past, maroder was seen selling accesses to various organizations’ networks, as well offering services of fund withdrawals from crypto exchanges, and even selling dumps of crypto exchanges. After conversing further with the seller, we managed to identify these victims to be two major universities, one in Israel and another in Germany.

Selling so called “access” is a rather fluid term and can enable a plethora of different actions for threat actors, depending on each of their goals. Though the threat actor cannot confirm whether the access is on an admin level or not, he does specify that this will enable Citrix access to the universities’ networks.



2 универа цитрикс

Автор: maroder, 21 июля в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики

maroder
гигабайт
Платная регистрация
4
102 публикации
Регистрация
18.07.2019 (ID: 94 453)
Деятельность
хакинг / hacking
Депозит
0.00000546 ₿

Опубликовано: 21 июля

продам 2 универа
израиль и германия
права не знаю
людям с репой дам доступ первый
чисто символически -400$ за оба

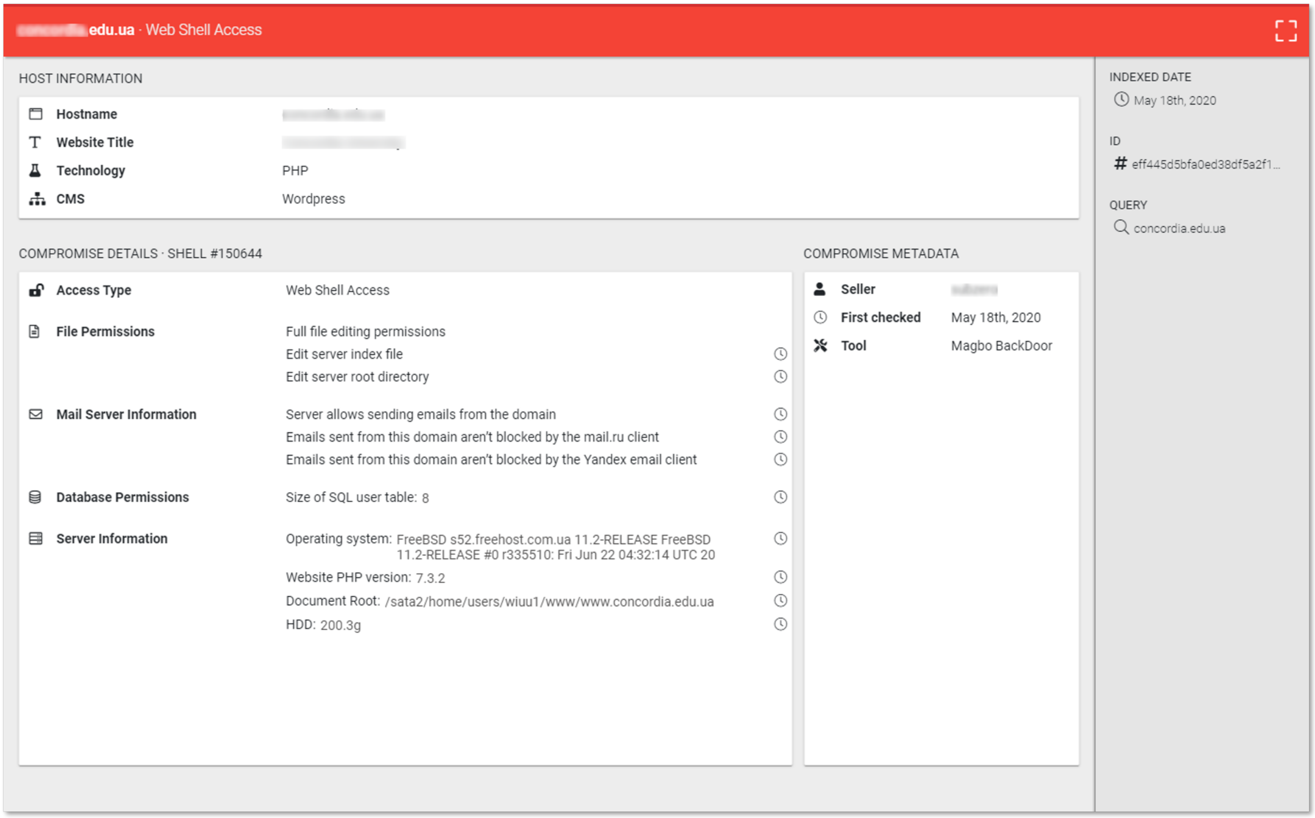
Translation from Russian:
Selling 2 uni
Israel and Germany
I do not know the rights
People with reputation will give access first
Purely symbolic – 400 $ for both

Maroder/ailing’s activities targeting education-related institutions didn’t stop there. Among one of his latest activities, from this past weekend, maroder was seen selling Citrix access to a school in UK with a current revenue of $100 million and more than 500 employees. Since this was only some days ago, the access again is undetermined however, maroder seems to be hunting down more targets of this type.

As mentioned above, compromised credentials can be an initial foothold for a larger attack. However, access to servers either via a direct attack or through a third party, can cause even more severe damage to victims.

By using DARKBEAST – KELA’s Darknet threat hunting technology – we ran a quick search for breached servers including the search term <university>, and were left with dozens of education-related institutions with compromised website access for sale.

Take this web shell access to a university's network for example. In the example below, upon purchase, buyers would gain immediate access to run a number of operations against the university such as editing files, editing the server's root directory, sending emails from the domain, and more. This web shell access can grant threat actors several different routes of attack once they've gotten in.



[redacted].edu.ua · Web Shell Access

HOST INFORMATION

Hostname	[redacted]
Website Title	[redacted]
Technology	PHP
CMS	Wordpress

INDEXED DATE
May 18th, 2020

ID
# eff445d5bfa0ed38df5a2f1...

QUERY
concordia.edu.ua

COMPROMISE DETAILS · SHELL #150644

Access Type	Web Shell Access
File Permissions	Full file editing permissions Edit server index file Edit server root directory
Mail Server Information	Server allows sending emails from the domain Emails sent from this domain aren't blocked by the mail.ru client Emails sent from this domain aren't blocked by the Yandex email client
Database Permissions	Size of SQL user table: 8
Server Information	Operating system: FreeBSD s52.freehost.com.ua 11.2-RELEASE FreeBSD 11.2-RELEASE #0 r335510: Fri Jun 22 04:32:14 UTC 20 Website PHP version: 7.3.2 Document Root: /sata2/home/users/wiuu1/www/www.concordia.edu.ua HDD: 200.3g

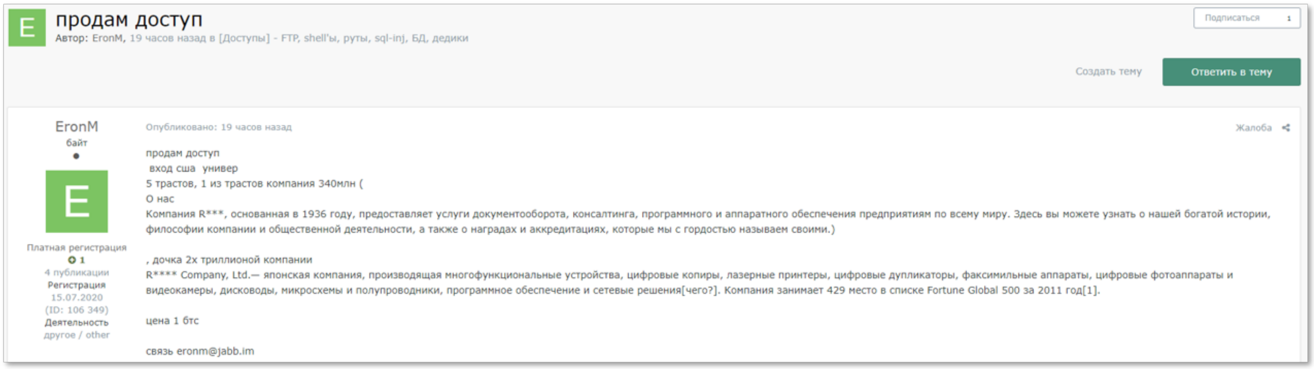
COMPROMISE METADATA

Seller	[redacted]
First checked	May 18th, 2020
Tool	Magbo BackDoor

Example of Web Shell Access for a [.]edu site for sale, captured by KELA's DARKBEAST.

At other times, we've seen universities being targeted as part of an attempted larger attack. On a well-known underground forum, we recently came across a threat actor posting VPN access for sale belonging to a US-based university, however when analyzing further content in the listing, most attention was pointing at the potential access it provides to a prominent US ISP and managed service company – the hosting service of the university. Upon further analysis we determined the access to this service company false, however would it have been true, it would have made the perfect use case for an example of something that can be used for deploying ransomware or other malware, stealing data, etc. Even though this was purely a marketing scheme, utilizing universities in an aim to attack a *bigger* target is a common occurrence.

Just last week, we noticed a threat actor selling access to another US-based university that was linked to many other big corporations. We found a threat actor identifying as "EronM" on a Russian-language cybercrime forum offering access to various organization across different fields. This threat actor was leveraging corporations linked to other larger organizations to maximize profits further than just the university itself. In this case, the university was linked by domain trust to a large Japanese company, which could mean that users in the university's trusted domain could authenticate to resources of the company. Cybercriminals could therefore leverage this access to compromise the larger company's network.



продам доступ

Автор: EronM, 19 часов назад в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики

EronM
байт
Платная регистрация
1
4 публикации
Регистрация
15.07.2020
(ID: 106 349)
Деятельность
другое / other

Опубликовано: 19 часов назад

продам доступ
 вход сша универ
5 трастов, 1 из трастов компания 340млн (
О нас
Компания R***, основанная в 1936 году, предоставляет услуги документооборота, консалтинга, программного и аппаратного обеспечения предприятиям по всему миру. Здесь вы можете узнать о нашей богатой истории, философии компании и общественной деятельности, а также о наградах и аккредитациях, которые мы с гордостью называем своими.)

, дочка 2х триллионой компании
R**** Company, Ltd.— японская компания, производящая многофункциональные устройства, цифровые копиры, лазерные принтеры, цифровые дупликаторы, факсимильные аппараты, цифровые фотоаппараты и видеокамеры, дисководы, микросхемы и полупроводники, программное обеспечение и сетевые решения[чего?]. Компания занимает 429 место в списке Fortune Global 500 за 2011 год[1].

цена 1 бтс

связь eronm@jabb.im

From Russian: "Selling access

Entry USA university

*5 trusts, 1 of the trusts is a company worth 340 million (about us: Company R***, established in 1936, offers document services, consulting, software and hardware to businesses around the world. This is where you can find out about our rich history, company philosophy and community activities, along with the awards and accreditations we're proud to call our own.)*

, a daughter company of a 2 trillion company

*R*** Company Ltd – a Japanese company producing multifunctional devices, digital copiers, laser printers, digital duplicators, fax machines, digital cameras and camcorders, disk drives, microcircuits and semiconductors, software and network solutions. The company was 429 in Fortune Global 500 for the year 2011[1]*

Price 1 btc"

Key Takeaways

As highlighted in several of the examples above, threats don't always necessarily stem from a direct target on the university itself, and even when direct attacks occur, they're not necessarily in an aim to attack the institution itself, rather it may be a part of a larger, more profitable attack. Nowadays, organizations, are obligated to look out for any potential threats on their entire supply chain in addition to their direct assets. The supply chain of organizations, though sometimes overlooked, can offer threat actors the perfect entry point into organizations. As seen in the ongoing weekly occurrences, institutions in the education sector are surely a target for many cybercriminals. These institutions should leverage advanced threat intelligence technologies to monitor their assets in real time, to ensure that they're maintaining a reduced attack surface and catching any potential threats at an early stage.