

Adversary Intelligence

Cyber Threats Targeting the Global Education Sector on the Rise

Author : Hansika Saxena

CloudSEK TRIAD (Threat Research & Information Analytics)

Table of Contents

Overview of Cyber Threats to the Global Education Sector	2
Cyber Attacks on Educational Institutions in 2021	4
Increase in Dark Web Activity Related to the Education Sector	13
Common Attack Vectors	14
Mitigation Measures	16
Create a Cyber Resilient Education Ecosystem	18
References	18
About CloudSEK	18

Overview of Cyber Threats to the Global Education Sector

The growing global education and training market (products and services, both online and offline) is expected to reach USD 7.3 trillion by 2025. This is 2x growth from 2019 to 2025. This promising outlook is predicated on the expanding education technology (ed tech) market, population growth, and increasing digital penetration in developing countries. Hence, it is no surprise that cybercriminals are gravitating towards entities and institutions in the sector.

XVigil data shows that ~5% of threats identified in 2021 targeted educational institutions. This can be attributed to:

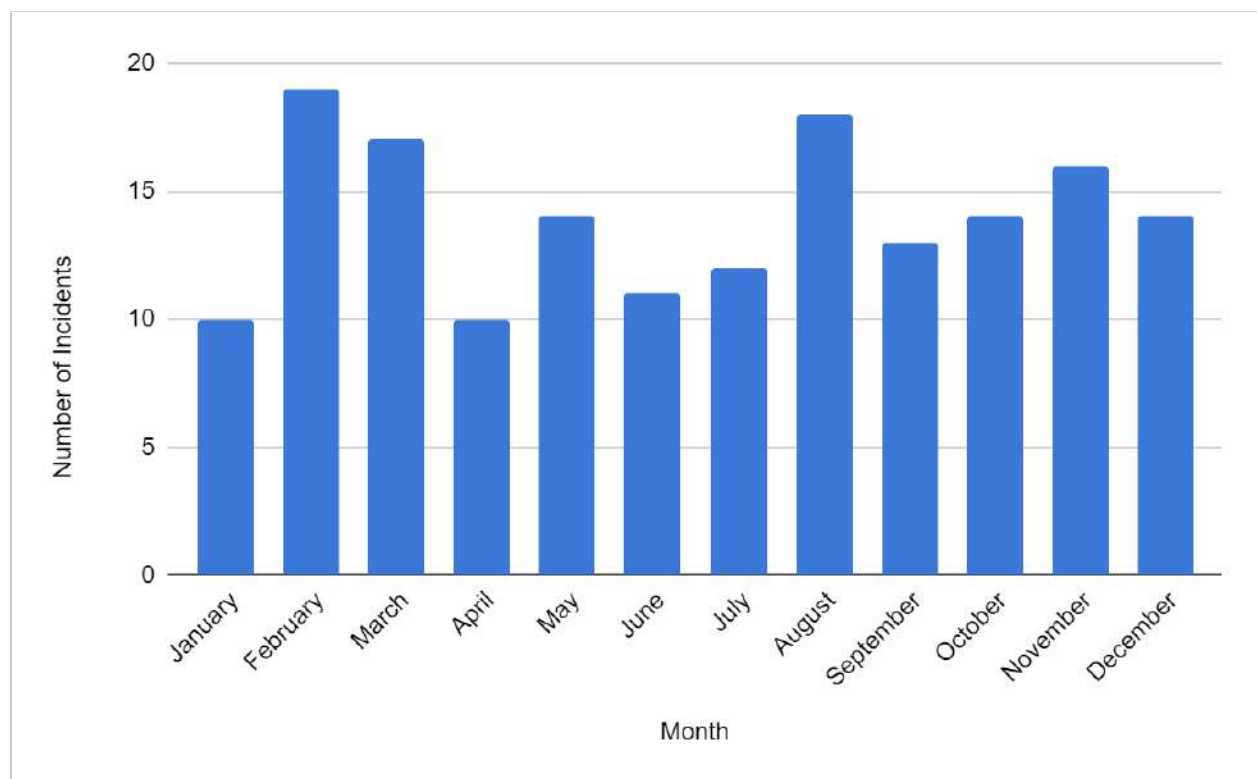
- Adoption of remote learning by schools, universities, and related entities, to combat the disruptions caused by the ongoing COVID-19 pandemic.
- Large-scale digitization of educational material, student data and documents, and administrative activities.
- Online learning platforms catering to the needs of everybody, ranging from preschool children to retired professionals.

In this report, we delve into:

- The major cyber attacks on prominent entities in the education sector in 2021
- Breakdown of the attacks by region and types of attacks
- Commonly used attack vectors
- Long-term impact of the attacks



Cyber Attacks on Educational Institutions in 2021



Monthly distribution of cyber attacks on educational institutions

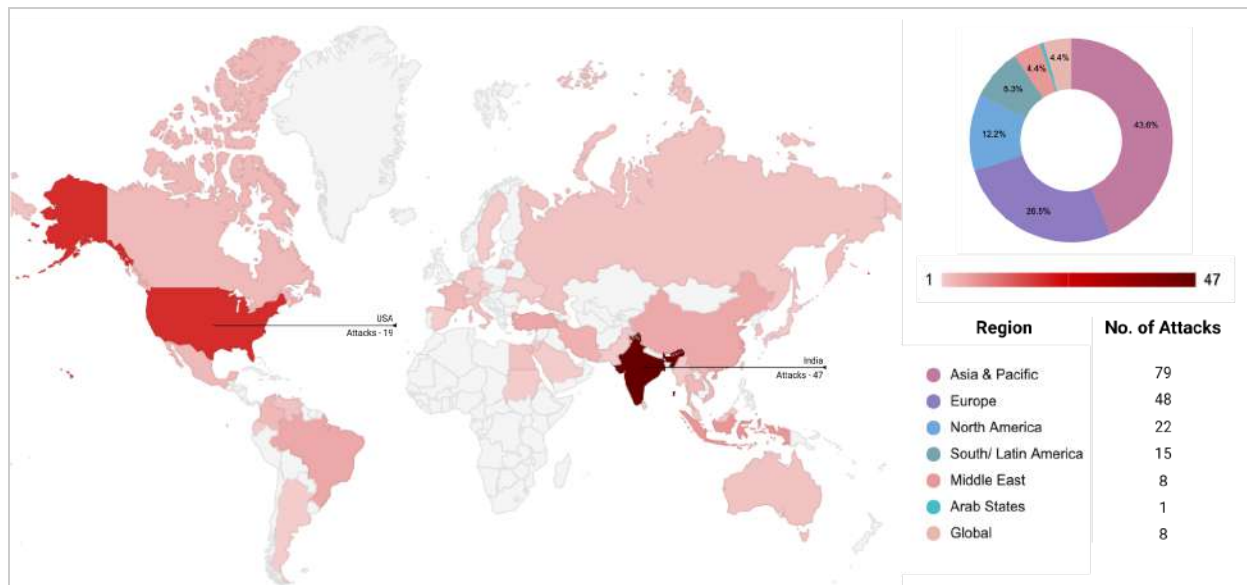
Most Targeted Regions

Data gathered by XVigil*, from multiple sources across the internet in 2021, shows that the majority of cyber incidents targeted education institutions in Asia & Pacific, followed by Europe, North America, South/ Latin America, and the Middle East.

India Emerges as a Prime Target for Threat Actors

Of the threats detected in Asia & Pacific, 58% of them were targeted at Indian or India-based educational institutions and online platforms*. This included attacks on Byju's, IIM Kozhikode, and Tamil Nadu's Directorate of Technical Education. After India, Indonesia comes a distant second, being the target of ~10% of the threats.

Overall, the USA was the second most affected country across the globe, with a total of 19 recorded incidents, accounting for 86% of the threats in North America. These include ransomware attacks on prestigious institutions such as Howard University and the University of California. In addition, high-risk API vulnerabilities were uncovered in Coursera, the massive open online course provider.



Map graph depicting the region wise number of recorded cyberattacks targeting the education sector

***Note:** The insights and distribution of threats by region are contingent on the presence of our clients in those regions.

Major Threat Actors

XVigil findings indicate that several major threat actors have been actively targeting the education industry around the world. These cybercriminals are actively leaking databases, accesses, vulnerabilities/exploits, and other information belonging to educational institutions, on cybercrime forums.

The graph below illustrates the number of threats by the top 5 threat actors most actively targeting the education sector. Among these, two threat actors who go by the handles “babam” and “Kristina”, posted more data leaks and accesses than any other threat actor.

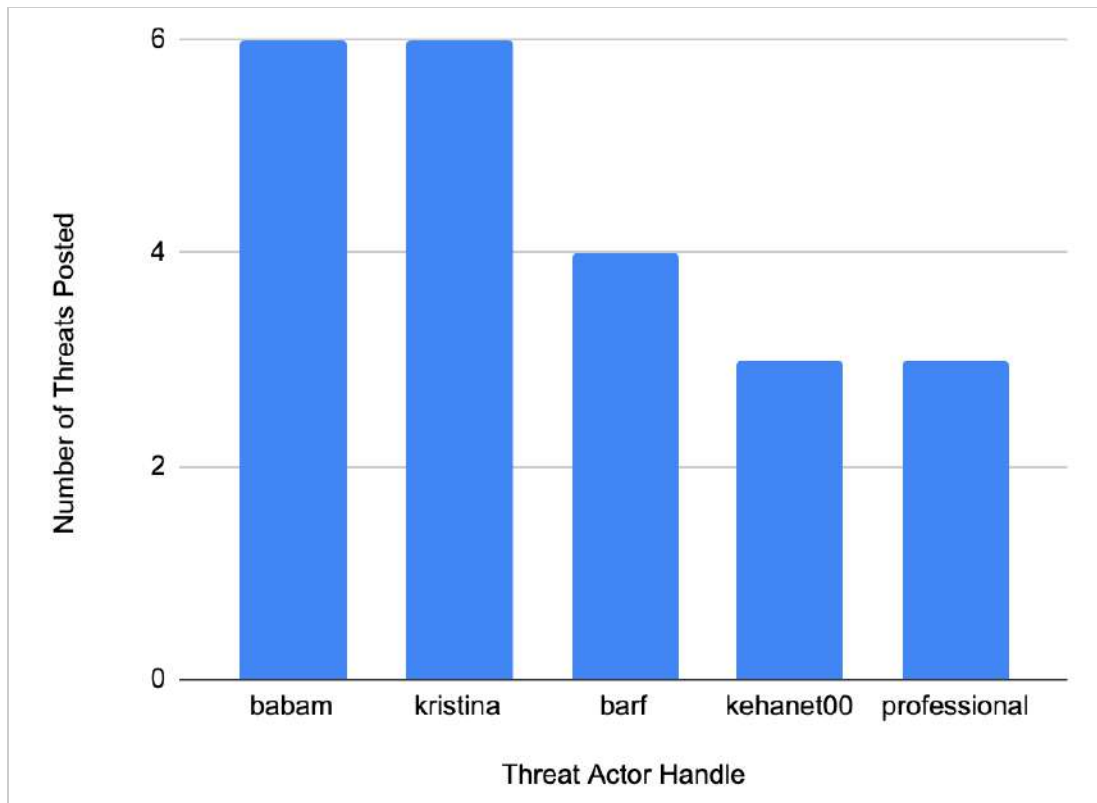
babam

- Babam is an [Initial Access Broker \(IAB\)](#) on a Russian cybercrime forum, active in the auction section of the forum.

- The actor specializes in selling different types of accesses (including Citrix, RDP, RDWeb, VPN) from across the world.
- The actor's history, and the types of accesses advertised, indicate that the actor generally extracts credentials from the logs of info stealer malware or bots.
- The actor had a high reputation on the forum, but due to payment related issues with some buyers, they were banned from the forum on 19 October 2021.

Kristina

- Kristina is a handle used by a threat group that was previously known as Kelvin Security team.
- The group uses targeted fuzzing and exploits common vulnerabilities to target victims. Being highly skilled in use of tools and having wide knowledge of various exploits, they share their list of tools and payloads for free.
- They typically target victims with common underlying technologies or infrastructure at any given time.
- The group doesn't shy away from attention and publicly shared information such as new exploits, targets, and databases on cybercrime forums and communication channels such as Telegram.
- Recently, they started their own data leak websites where other threat actors can come and share databases.



Top 5 threat actors targeting the education sector

Commonly Sought After Data Types

Databases and accesses were the most commonly sought after data types, with ~73% of reported cases involving the leak or sale of databases belonging to educational institutions and learning platforms.

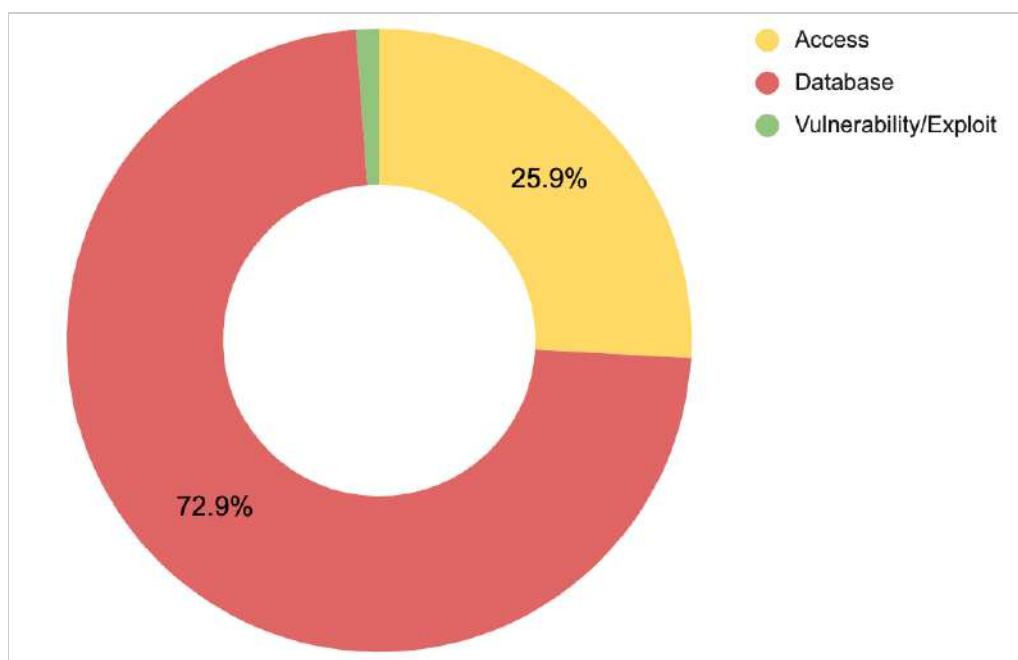
These databases primarily contain:

- Personally Identifiable Information (PII), of students and their families, such as:
 - Name
 - Date of Birth
 - Email ID
 - Phone numbers
 - Address
- Website user records and credentials
- Examination results and scores

In 26% of the threats, actors were selling or sharing accesses to educational organizations'

- Citrix instances
- SMTP servers

- API credentials
- RDP (Remote Desktop Protocol)
- RD Web (Remote Desktop Web Access)




Type of data posted on underground forums in posts related to the education sector

Increase in Dark Web Activity Related to the Education Sector

CAT 2020 Student Information and Scores

- On 12 May 2021, a threat actor leaked 190,000 PII records of students who appeared for the 2020 CAT (Common Admission Test) exam, along with their scores.
- CAT is a computer-based test for admission to graduate management programs.

CAT 2020 - India's Entrance Exam for MBA 190,000 records
by [redacted] - 6 hours ago New Reply



GOD User

Posts: 24
Threads: 4
Joined: Nov 2018
Reputation: 100
2 YEARS OF SERVICE

6 hours ago

India's Common Aptitude Test (CAT) 2020 database with fields such as Name, Phone, Email, Address, Score, and other fields with over 190,000 records.

Sample:
Click Here [redacted]

Hidden Content

Unlock for 8 credits

Format: Excel

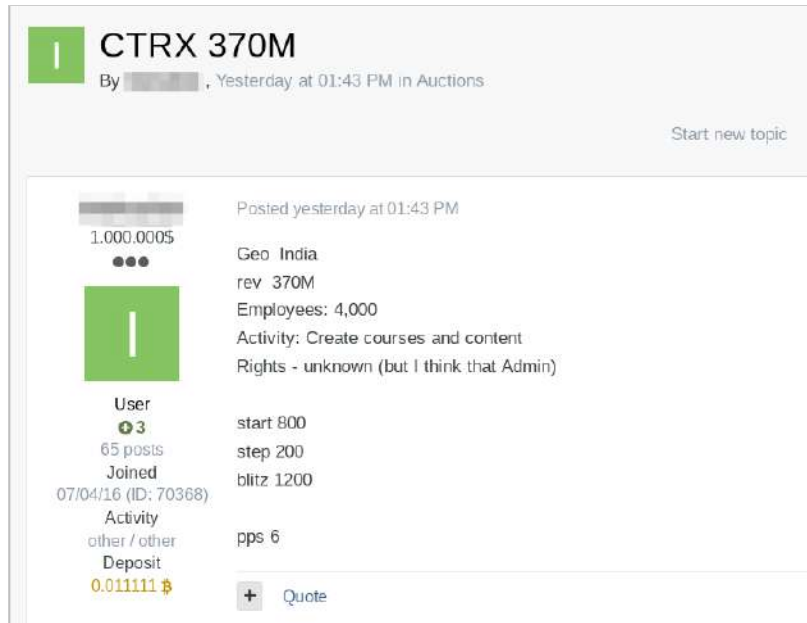
PM Find
Reply Quote Report

NAME	DOB	EMAIL	MOBILE	GENDER	ADDRESS 1	ADDRESS 2
A.S.	01	mail.com		Male	51/	
A.S.	21	.com		Male	da/	
A.A.	08	.com		Male	183	
A.A.	25	om		Male	17-	
A.A.	03	mail.com		Male	R N	
A.A.	14	m		Female	I bi	
A.A.	20	om		Male	Typ	
A.A.	25	om		Female	Fla	
A.A.	15	om		Female	NE	
A.A.	10	m		Male	D-3	
A.A.	14	mail.com		Male	52-	
A.A.	15	n		Male	HIG	
A.A.	20	ail.com		Male	Hot	
A.A.	23	com		Female	C40	
A.A.	33	mail.com		Female	39/	
A.A.	08	il.com		Female	H.A	
A.A.	24			Male	C-3	
A.A.	20	@gmail.com		Male	A A	
A.A.	25	m		Male	18	
A.B.	21	mail.com		Male	4/2	
A.B.	10	n		Male	Fla	

Threat actor sharing the 2020 CAT exam database

Databases and Citrix Access belonging to BYJU'S

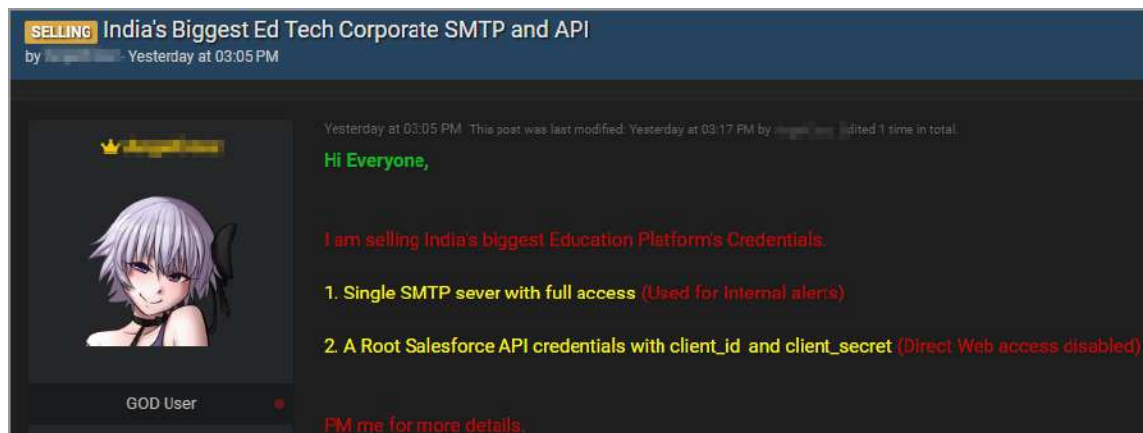
- On 10 May 2021, a threat actor advertised Citrix access to BYJU'S, an Indian multinational educational technology company, headquartered in Bangalore.
- In addition, another threat actor leaked BYJU's databases. The data was purportedly exposed due to an unprotected SalesKen server that had been left unsecured, without a password, since 14 June 2021. The databases contained:
 - PII and sensitive information related to students, parents, and instructors
 - Conversation logs between parents and staff, including remarks about their children.
 - Copies of emails with codes to reset user accounts and internal Salesken.ai data



Threat actor selling Citrix access to BYJU'S

Access to India's Largest Ed Tech Platform

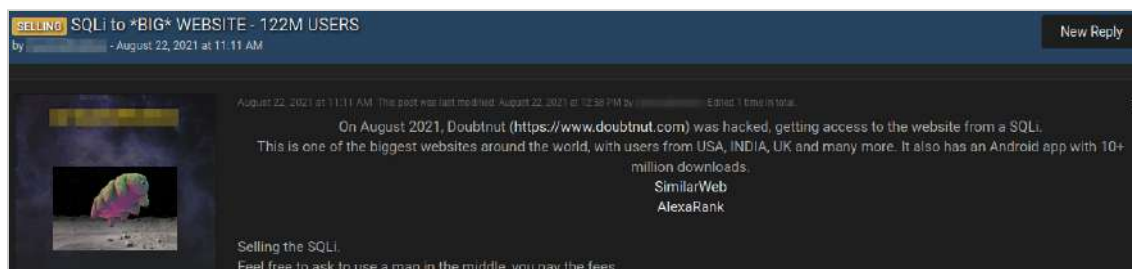
- On 1 September 2021, a threat actor shared a post advertising access to the SMTP server and API credentials of allegedly the largest Indian ed tech platform.



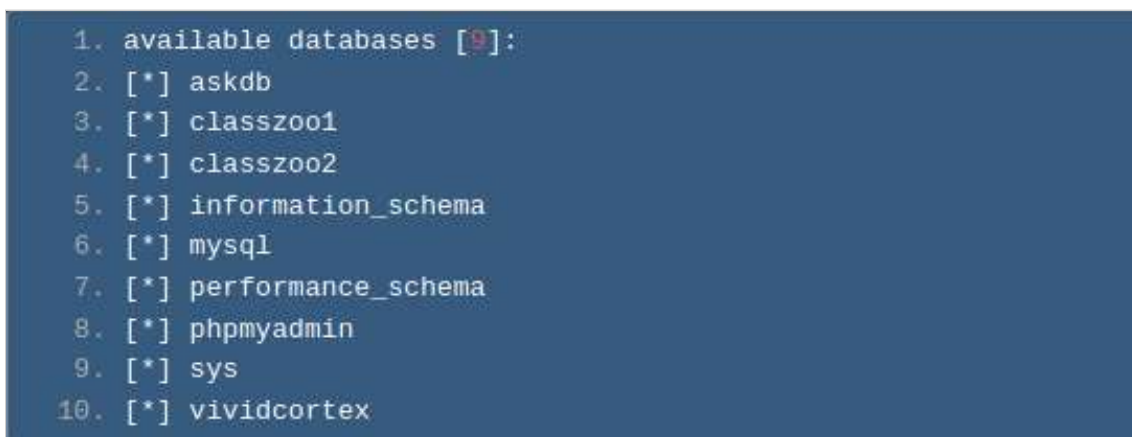
Threat actor selling access to India's Largest Ed-tech platform

SQLi Vulnerability in Indian Ed Tech App DoubtNut

- On 23 August 2021, a threat actor published a post advertising an SQLi vulnerability in Doubtnut, an Indian educational app started by Tanushree Nagori and Aditya Shankar in 2016.
- The actor claimed that the alleged SQLi provides access to 122 million user records.



Threat actor selling SQLi in Doubtnut



Databases exposed due to the SQLi in Doubtnut

IIM Kozhikode Website User Records

- On 2 August 2021, a threat actor shared the website user records from the official website of Indian Institute of Management Kozhikode, an autonomous public business school located in Calicut, Kerala.
- The institute is fifth out of the 20 IIMs in India.



Threat actor exposing website user records of IIM Kozhikode

age_limit.csv	421 bytes
AllQualification.csv	1.1 kB
appln_draft.csv	37 bytes
appln_experience.csv	6.0 MB
appln_personaldata.csv	3.5 MB
appln_photo.csv	238.7 kB
appln_qualifications.csv	3.8 MB
appln_summary.csv	1.4 MB
category.csv	49 bytes
list.csv	9.7 kB
list_old.csv	8.9 kB
Paymentconfirm.csv	309.9 kB

CSV files contained in the IIM Kozhikode data leak

Citrix Access to American Public School District

- On 7 July 2021, a threat actor auctioned the Citrix access to an American public school district having a revenue of USD 209 Million.
- The threat actor claimed to have access, along with user rights, to 3 PCs belonging to the school's network.

W Access USA Revenue: \$ 209 Million 3pc
 By **byte** 19 hours ago in Auctions

byte Posted 19 hours ago

Revenue: \$209 Million
 Public school district
 Country: USA
 3 pc access
 Citrix/User
 Start \$ 150
 Step 50 \$
 Blitz \$ 300

Paid registration
 0
 1 post

Threat actor selling Citrix access to American Publish School District

RDP Access to Multiple Educational Institutions

- On 22 August 2021, a threat actor advertised RDP, RDWEB, and Citrix access to multiple educational institutions.
- Interested buyers were directed to the seller's Telegram channel.

SELLING rdp, rdweb, citrix access
 by **New User** Yesterday at 06:13 PM

New User Yesterday at 06:13 PM

Sale of accessess rdweb, citrix ..

there are about 10 accessess. there will be more soon.
 for all questions write to telegram: @akshay...

MEMBER

Posts 37
 Threads 13
 Joined Feb 2019
 Reputation 0
 2 YEARS OF SERVICE

PM Find

Reply Quote Report

Threat actor selling RDP, RDWeb, & Citrix access to multiple educational institutions

Database of Aakash Educational Services

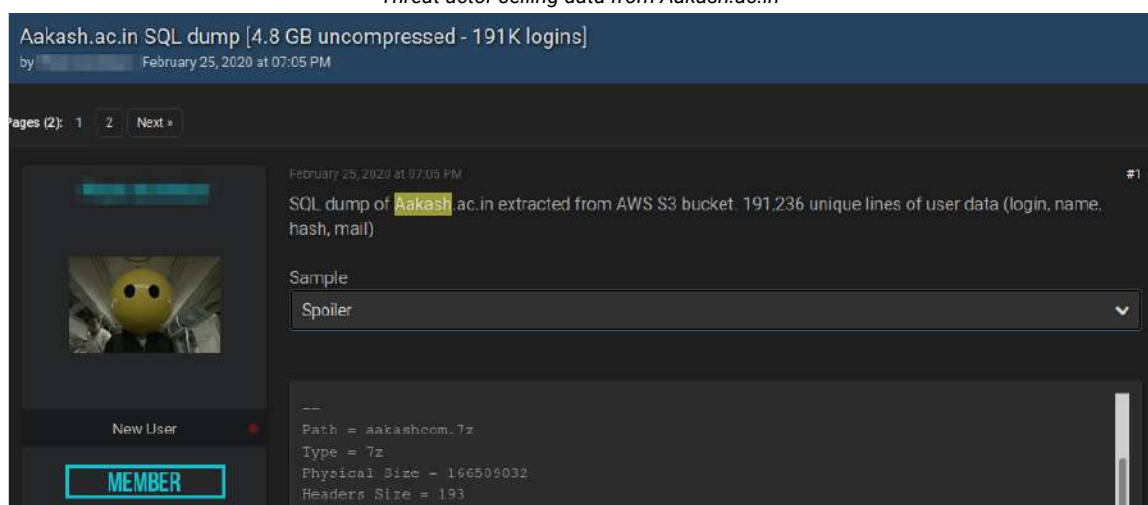
- On 18 December 2021, a threat actor shared the database from Aakash Educational Services Limited (AESL), a leading test-prep company in India that provides test preparatory services for

students preparing for Medical and Engineering entrance exams, School/Board exams, and competitive exams such as NTSE, KVPY, and Olympiads.

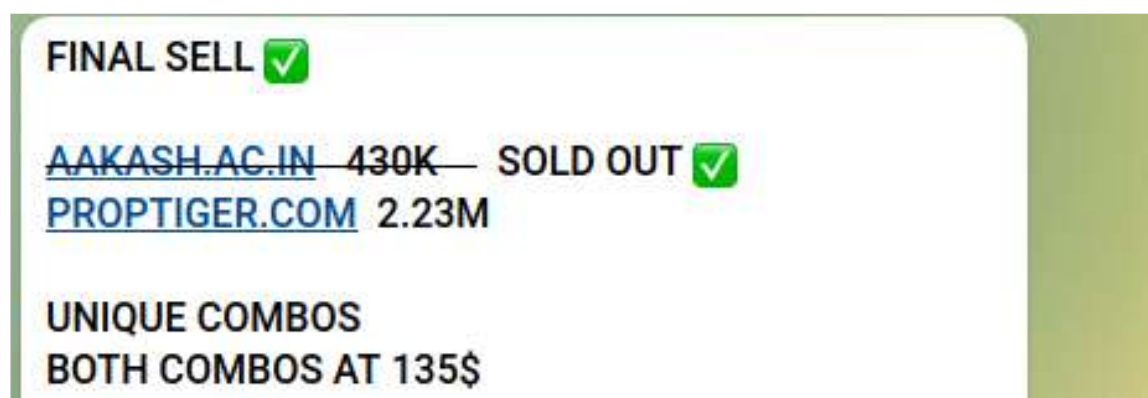
- The actor was found selling this data on multiple platforms.



Threat actor selling data from Aakash.ac.in



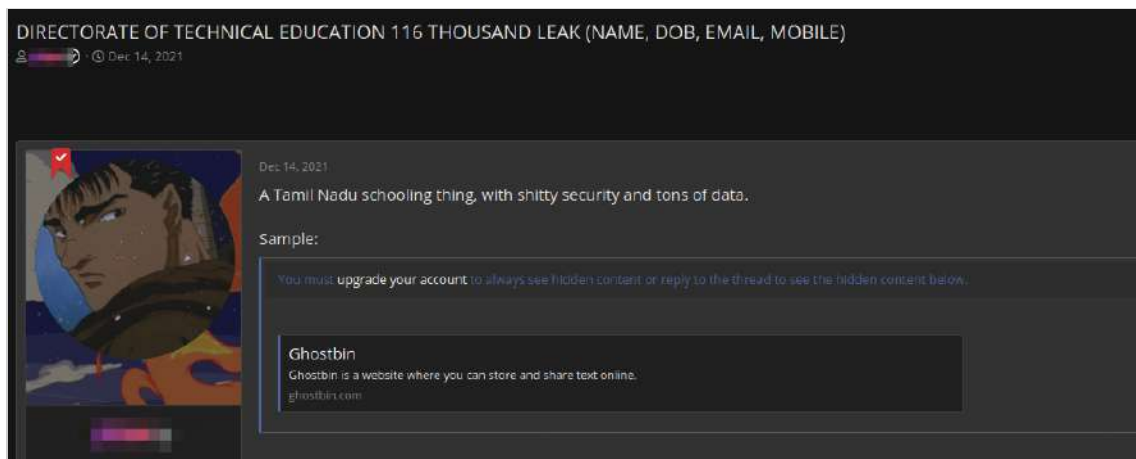
Threat actor sharing the SQL data dump from Aakash.ac.in



Threat actor selling data from Aakash.ac.in on Telegram channel

PII from Tamil Nadu's Directorate of Technical Education

- On 14 December 2021, a threat actor shared the PII from Tamil Nadu's Directorate of Technical Education.



Threat actor sharing PII from Tamil Nadu's Directorate of Technical Education

INSERT	ident info	b code	category	b, 'gender	'email	ity, 'nativ	on', 'commu
caste	parent occu	state	hsc in	xam', 'name	'year of	hsc reg no	'eleventh
physic	physic t,	_m, 'ches	maths m,	optional s	't, 'ann	'aicte_tf	'fg distr
fg oc	d fg, 'sa	oved, 're	approved	'VALUES			
('0001	10001', 'P	'VISHAL	03-05-31',	76899000	'yahoo.co	'TN', 'HI	'PRIVATE
TAMIL	HEKNAI', 1,	TN-Tamil	f Higher S	cation',	2006', 'G	89, 100, 89	0, 90, 100,
NULL,	0, 1, 1,	},					
('0001	1112', 'NP	A JUMANA	'2002-06-	'770849	hajumanab	'INDIAN',	DM', 'OC',
'PROFI	'TAMILNAC	ELVELI',	Others',	3097', 'GE	8, 100, 0	100, 77, 10	'0, '0', '0'
'1,							
('0001	1170', 'NP	N VIJAYAN	-08-04', 'I	563262', 'I	ananbil30	'OTHERS',	'OC', 'I,
'PROFI	'Others',	1, 'CBSE	'2020',	GENERAL',	91, 100,	0, 0, 0, NU	'0, 1, 1,
('0001	1266', 'NP	I G K', 'I	'FEMALE',	'gkjanu	.com', 'O	'HINDHU'	PRIVATE', 'C
'OTHEF	'OTHERS', 'OI	20', '1900	'GENERAL',	69, 100,	100, 0,	'0', '0', '0,	'OC', 'I,
('0001	1326', 'NP	ARTH K NA	'2-02-21',	8305516',	agarakjgm	'OTHERS', 'OT	'OC', 'I,
'PROFI	'Others',	1, 'CBSE	'2020',	GENERAL',	90, 100,	100, 0, 0,	'0', '0, 1,
'1,							
('0001	1496', 'NP	GAM NEELA	I', '2001-	ALE', '994	rumugen 1	'INDIAN'	HU', 'OC',
'PROFI	'TAMILNAC	HIRAPPALL	'Others	27609203,	1, 66, 10	30, 100, 70	NULL, 0, 'I,
1, 1,							
('0001	200969',	'RINZA	'2003-0	LE', '7440	mzofathim	.com', 'INDI	USLIM', 'BO
Labba3	g Rowthar	yar', 'OTI	LNADU', 'CI	'CBSE', 'O	0', '2000	SRAL', 1, 94	0, 95, 100,
3, 1,	ENNAI', 'I	'1, 'I					
('0001	202202',	'KARPA	'2003-05-2	'9080530	kalki50gm	INDIAN', 'TN	'BC', '230-7
includ	or Thuluv	'STATE	E', 'TAMIL	R', 0, 'CB	'2020'	'GENERAL'	95, 100, 95
100, 4	'CHENNAI'	1, 'I					
('0001	210037',	'SHIRI	'2002-10-1	'755025256	aran18100	'INDIAN',	'SC', '80-
Parays	'm', 'STATE	OYEE', 'TI	CHENGALPAT	E', 'Other	'20002882	'1, 99, 10	9, 100, 99,
0, 0,	'0, 1,	'I,					
('0001	220506',	'M KARI	-03-22', 'I	01133998',	Sgmail.co	'TN', 'HI	NC', '143-Va
Kshati	ding Vanni	ya,Vannia	under of K	ach, Pall	Kshatriy	'TAMILNA	DR', 0, 'CB
Centr	f Secondar	n', '2020	'GENERAL'	00, 99, 100	90, 100,	'CHENNAI'	'I, 'I,
('0001	222652',	'B R Si	'2002-04	'99400814	nbs@gmail	IAN', 'TN	'500-Othe
'PROFI	'TAMILNAC	AI', 0, 'I	rs', '2020	'GENERAL'	00, 90, 1	97, 100, 5	HENNAI', 'I,

Sample of the data from Tamil Nadu's Directorate of Technical Education

Common Attack Vectors

Our analysis shows that the following are immediate challenges to the education sector:

Ransomware

- Malicious actors have long used ransomware as a means of extortion. Several colleges, schools, and universities have been targeted by ransomware attacks, with disastrous results.

- According to the FBI, in August and September of 2020, K-12 schools were involved in 57% of all ransomware incidents, over twice the number of school ransomware attacks reported in the first months of the year. The average ransom was ~USD 50,000, but the largest was ~USD 1.4 million.
- A classic example of this was the ransomware attack on Howard University, which came to light on 03 September 2021.

Vulnerabilities and Exploits

- Many threat actor groups begin their attack on any target organization by exploiting the publically known software or web vulnerabilities.
- 2021 witnessed the discovery of some highly critical vulnerabilities such as Log4j, PrintNightmare, etc., which were actively being exploited across the globe to compromise organizations in all sectors.
- A few prominent attacks that exploited vulnerabilities in education institutions include:
 - Several API vulnerabilities in Coursera including:
 - Enumeration via password reset function error
 - Resource limitations with both a GraphQL and a REST API
 - GraphQL misconfiguration.
 - Broken Object Level Authorization (BOLA) security flaw
 - Dallas ISD, a network of approximately 230 schools with a total enrollment of 155,861 students was breached by two of their students. The breach exposed:
 - Student grade information
 - Confidential information of employees, students, and parents
 - Computer vulnerability reports
 - A Zero-day vulnerability in the File Transfer Appliance (FTA) product of Accellion, a technology company based in the United States, resulted in data breaches at government and private entities across the globe. This included three prominent universities:
 - Stanford University
 - University of Maryland, Baltimore
 - University of California, Berkeley

Mitigation Measures

Given the size and impact of the education sector, it is critical for institutions, students, parents, teachers, and the government to ensure that the information gathered and stored is not leaked and exploited by cybercriminals. To ensure this, we recommend that:

- Educational institutions and related government entities:
 - Create awareness among users regarding cyber-attacks, online scams, and phishing campaigns
 - Enact strong password policies and enable multi-factor authentication (MFA)
 - Update and patch software, systems, and networks on a regular basis
 - Maintain multiple backups, both online and offline, in separate and secure locations
 - Monitor logs for unusual traffic and activity to websites and other applications
 - Block illegitimate IP addresses and deactivate port forwarding using network firewalls
 - Perform real-time monitoring of the internet to identify and mitigate low-hanging threats, such as misconfigured apps, exposed data, and leaked accesses, that are leveraged by cybercriminals to carry out large scale attacks.
- Students, parents, faculty, and staff should:
 - Avoid clicking on suspicious emails, messages, and links
 - Not download or install unverified apps
 - Use strong passwords and enable multi-factor authentication (MFA) across accounts

Create a Cyber Resilient Education Ecosystem

The COVID-19 pandemic and the related disruptions have overhauled traditional learning spaces and redefined how the stakeholders involved interact, communicate, and collaborate. Online classes, along with the mushrooming of ed tech platforms, has made previously inaccessible information open to cybercriminals. These attacks have been exacerbated by the sector's dependence on antiquated technological infrastructure.

This is especially concerning, given that a large portion of students are under the age of consent and have limited awareness about how their data can be misused. Hence it is critical for educational institutions, ed tech platforms, and governments to prioritize the cybersecurity posture of the sector by leveraging automated threat monitoring, building resilient infrastructure, and adopting safe cybersecurity practices.

References

- [Indian tech startup exposed Byju's student data](#)
- [Howard University cancels classes after ransomware attack](#)
- [List of Data Breaches in the Education Sector](#)
- [Coursera API vulnerabilities disclosed by researchers](#)
- [WFAA reveals the masterminds behind last year's Dallas ISD cyber breach](#)
- [Data from three universities published online in latest Accellion-related data breach](#)
- [Global EdTech Market to reach \\$404B by 2025 - 16.3% CAGR](#)

About CloudSEK

CloudSEK is an AI-driven Digital Risk Management Enterprise. CloudSEK's XVigil platform helps clients assess their security posture in real-time from the perspective of an attacker. XVigil scours thousands of sources (across the surface, deep and dark web), to detect cyber threats, data leaks, brand threats, identity thefts, etc. To learn more about how the CloudSEK XVigil platform can strengthen your external security posture and deliver value from Day 1, visit <https://cloudsek.com/> or drop a note to sales@cloudsek.com.