

# Biggest Education Industry Attacks in 2024

 [socradar.io/biggest-education-industry-attacks-in-2024/](https://socradar.io/biggest-education-industry-attacks-in-2024/)

October 21, 2024

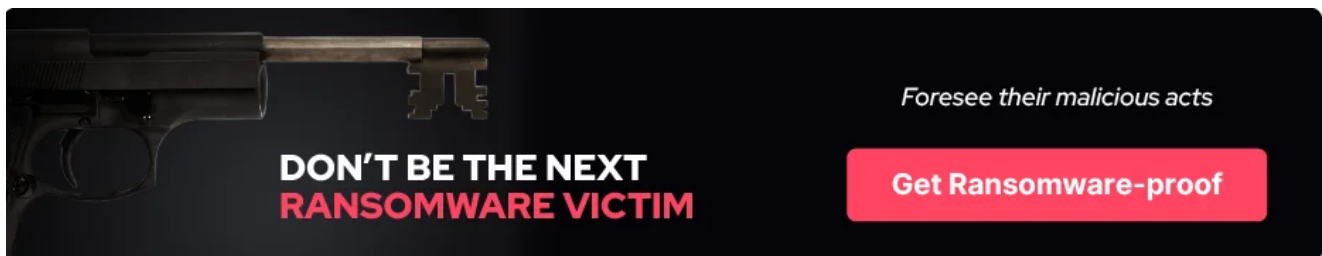
 SOCRadar® Cyber Intelligence Inc. | Biggest Education Industry Attacks in 2024

The education sector is increasingly becoming a top target for cybercriminals, with a noticeable rise in cyberattacks aimed at schools and universities throughout 2024. As institutions continue their digital transformation and integrate more technology into classrooms, they expose themselves to new security threats.

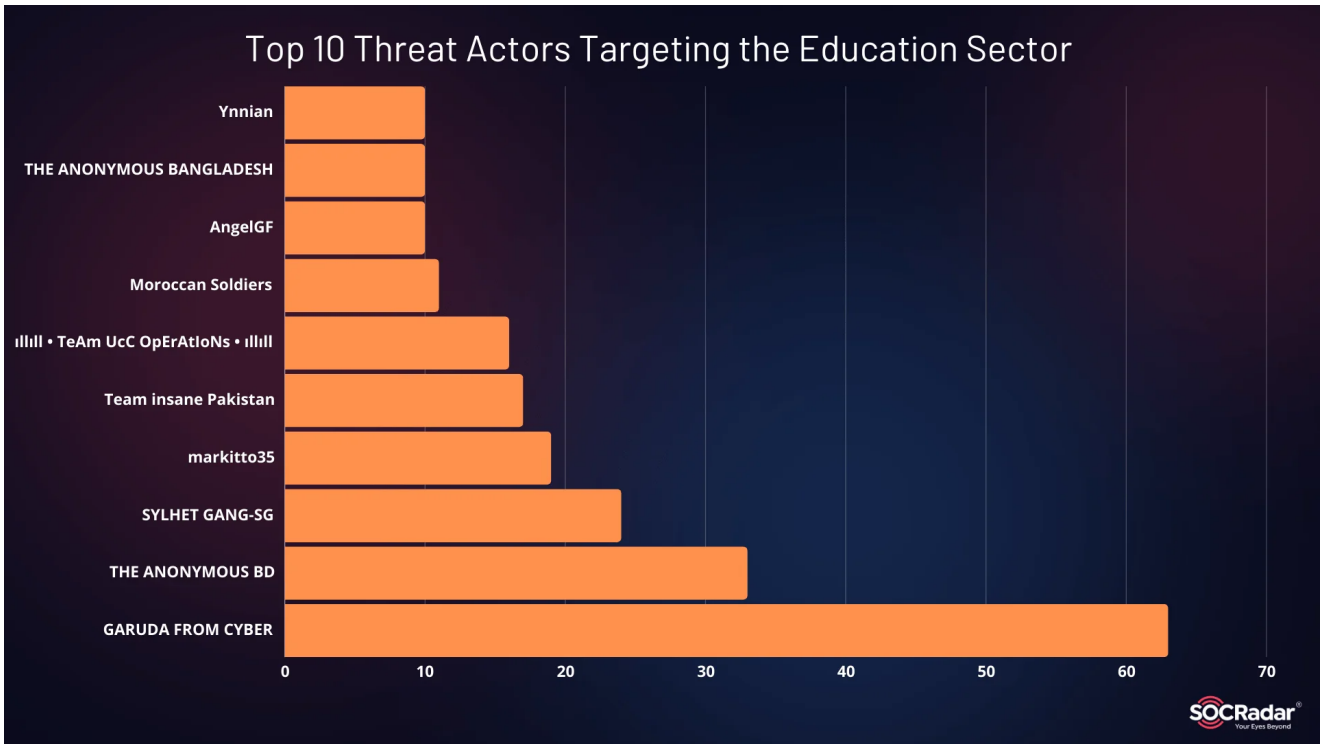
This year, the education sector saw many ransomware incidents, data breaches, and phishing attacks, exploiting outdated systems and insufficient cybersecurity practices. These cyberattacks disrupt learning environments and risk exposing the sensitive personal data of students and staff.

## Cyber Threat Landscape in Education

The education industry has become an increasingly attractive target for cybercriminals in 2024, with a variety of threat actors actively exploiting vulnerabilities in this sector. Microsoft's [Cyber Signals report](#) also highlighted the severity of the issue, revealing a rising trend in cyberattacks targeting educational institutions globally. Over the past year, schools faced threats like ransomware and phishing, which are fueled by the sector's reliance on outdated infrastructure and lack of robust security measures.

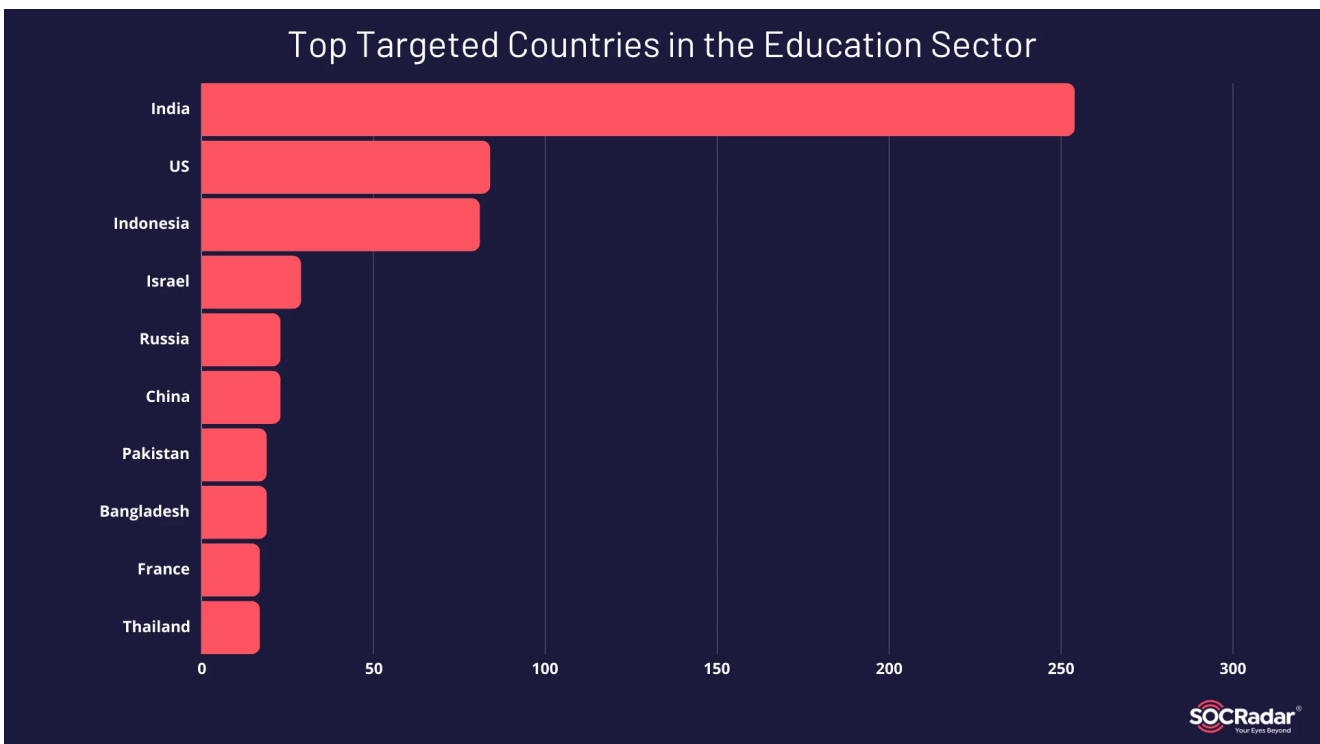


According to the report, attackers focus on exploiting these vulnerabilities to steal sensitive data, disrupt operations, and demand hefty ransoms, further crippling already strained IT budgets. Notably, the education sector is becoming a prime target due to the extensive personal information stored in its systems and the high potential for operational disruption. So, let's see the threat landscape further with this year's data so far.



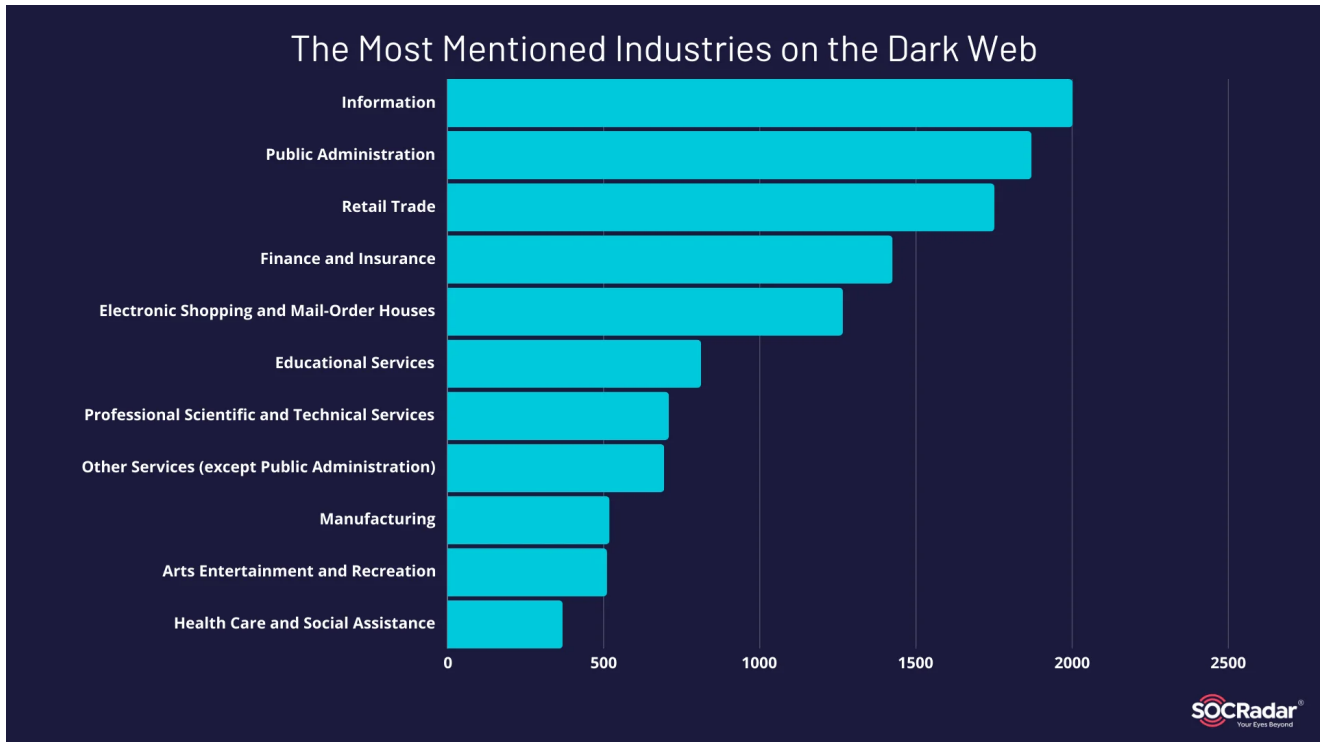
Top threat actors targeting the education industry

This year's data highlights the prominence of hactivist groups. Many of these groups, largely from South Asian countries, have targeted India's education sector, with most attacks involving data leaks.



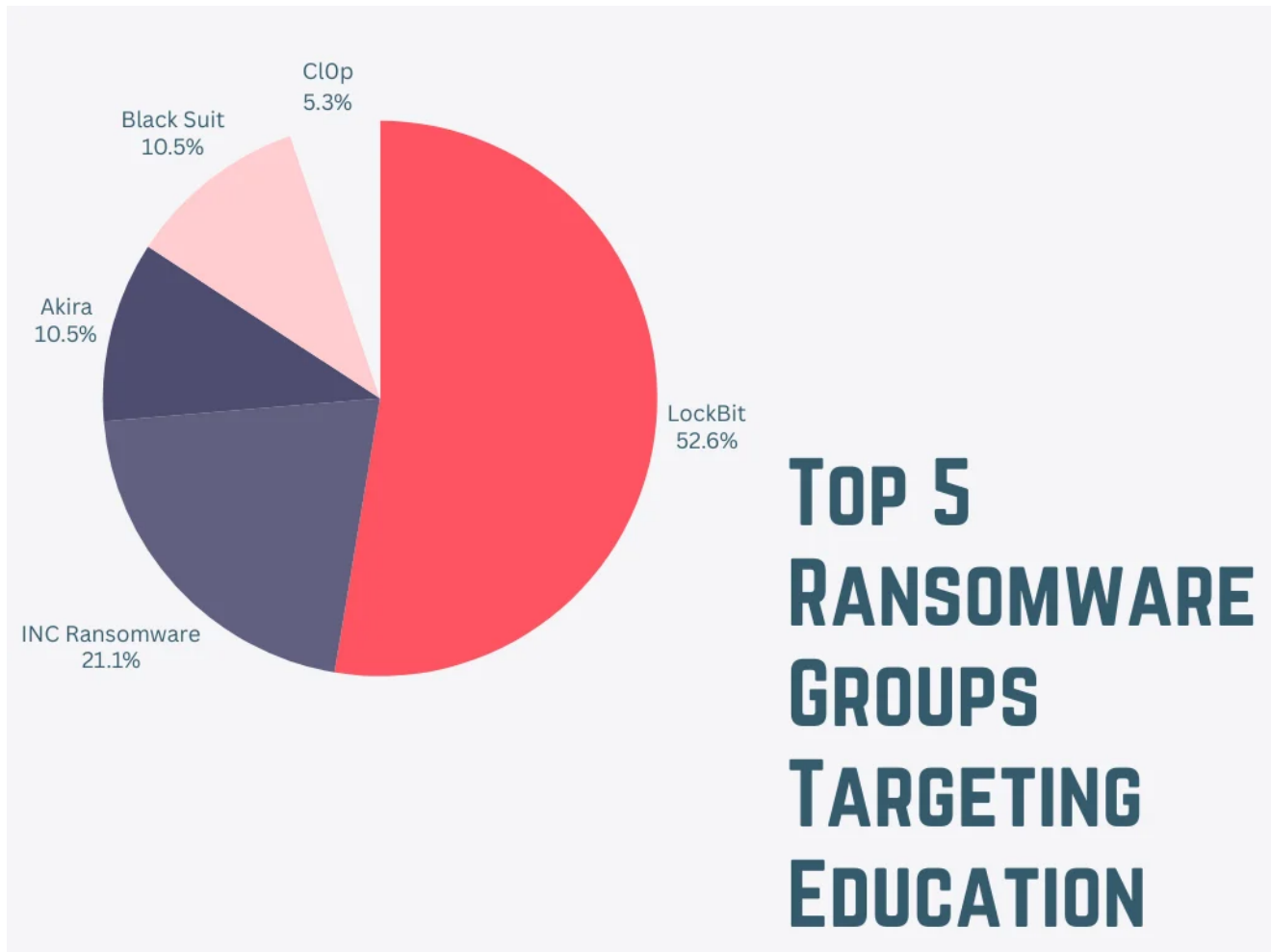
Top targeted countries in first 3 quarters of 2024

The strong focus on India stems from two key factors: South Asian groups, particularly those with Islamic leanings, view India as a primary cyber target, and the country's education sector has notable cybersecurity weaknesses. Given India's perceived bias in the Israel-Palestine conflict, it is unsurprising that hacktivists from neighboring countries have exploited these vulnerabilities.



Most mentioned industries in first 3 quarters of 2024

When we examine the data across various industries, it's clear that the education sector continues to rank high in terms of cyberattack targets. Despite not being the most lucrative sector for financial gain, the sensitive data stored within educational institutions and their comparatively weaker defenses make them particularly appealing to cybercriminals. The combination of valuable personal information and the ease of exploiting outdated systems allows this sector to stand out among dozens, if not hundreds, of other industries.



Ransomware groups that have focused on the education sector so far this year

Beyond hacktivism, ransomware poses another significant threat. LockBit, though diminished in power, has continued to target education-related institutions, seemingly unconcerned with financial gain. Throughout the year, the educational services sector has repeatedly been hit by ransomware attacks, attracting the attention of other groups as well.

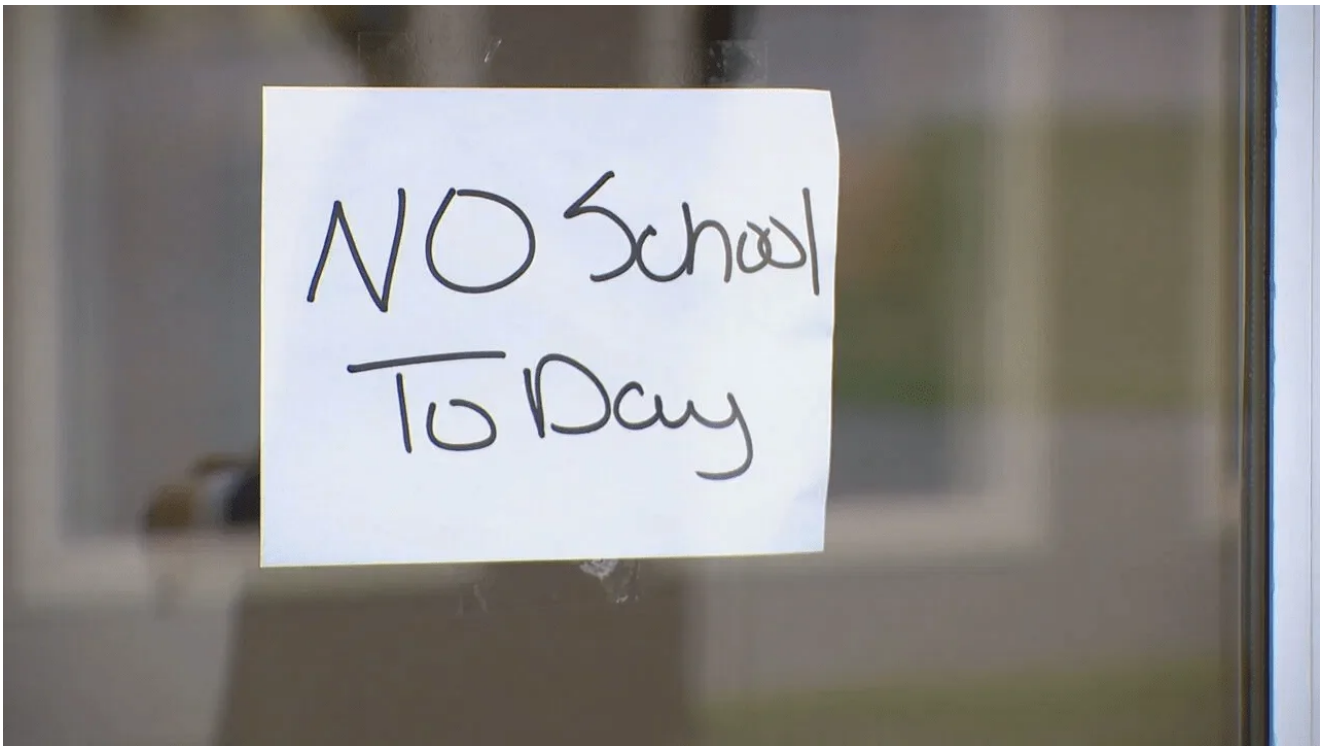
In particular, the US education sector has faced severe disruptions due to ransomware this year, with schools being forced to close, sensitive data allegedly leaked, and a range of other issues arising. We'll explore these incidents further in the list below.

*The following list is not arranged by significance or impact, but rather aims to illustrate the diverse range of cyber attacks and methods that have targeted the education sector this year.*

## 1. Highline Public Schools Hit by Ransomware Attack, Shuts Down Operations

Highline Public Schools, serving over **17,500 students** across 34 schools in Washington State, confirmed a ransomware attack in early September that forced a district-wide shutdown. The attack, discovered on September 7, led to the closure of schools and

suspension of activities. The district is still working to restore its network, with plans to re-image all staff and student devices beginning October 14, excluding Chromebooks and Apple devices, which only require password resets.



*Highline Public Schools canceled classes due to a cyberattack (Source: [KOMO News](#))*

No details about the ransomware group involved or potential data exposure have been released yet, but as a precaution, staff are offered one year of free credit and identity monitoring. Highline is working with federal and state authorities and has engaged third-party cybersecurity specialists to investigate the breach, but further details on law enforcement involvement remain undisclosed.

## **2. Toronto District School Board Confirms Student Data Breach Following Ransomware Attack**

---

The Toronto District School Board (TDSB) confirmed in August that student information was compromised in a ransomware attack discovered in June. Initially, TDSB stated that the attack targeted a separate technology testing environment. The board oversees 582 schools and approximately 235,000 students. This week, TDSB revealed that data from some students in the 2023/2024 school year, including names, grades, email addresses, and birth dates, was affected.

Deadline: 12 Sep, 2024 16:28:16 UTC

[no logo]

**tdsb.on.ca**

The Toronto District School Board, also known under the acronym of TDSB, is the largest school Board in Canada and the fourth largest in North America

UPLOADED: 29 AUG, 2024 15:28 UTC

UPDATED: 29 AUG, 2024 15:28 UTC

\*Download archives from reserve servers

LINK #1

LINK #2

LINK #3

LINK #4

LINK #5

LINK #6

LINK #7

LINK #8

LINK #9

LINK #10

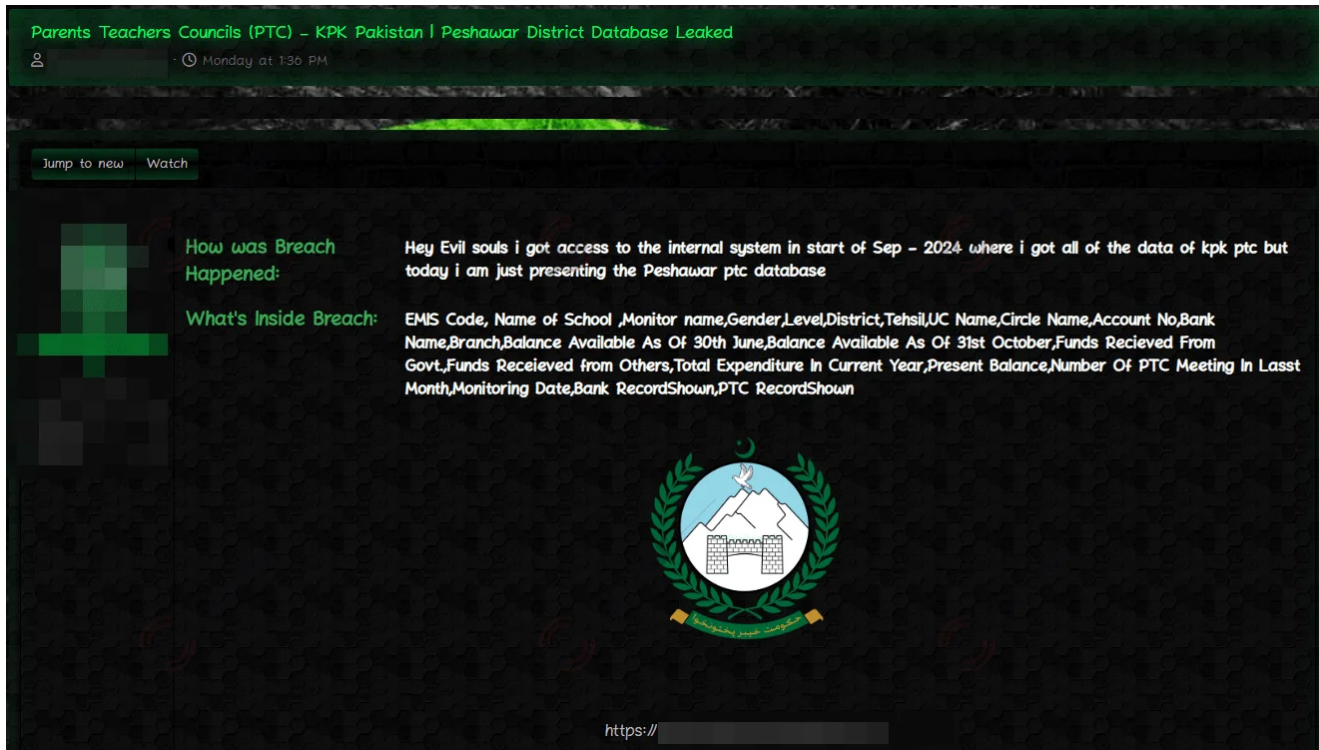
Allegedly published data of TDSB after the deadline on LockBit's leak site

Although TDSB assured that the risk to students is low and no data has been publicly disclosed, the LockBit ransomware group claimed responsibility for the attack, demanding a ransom with a **13-day deadline**. TDSB did not comment on the LockBit post but defended its response, emphasizing security improvements and collaboration with law enforcement. At the time of the incident, the school board was advised by Ontario's Information and Privacy Commissioner to notify the public about the data breach so affected individuals could file complaints.

### 3. Alleged Data Leak of Khyber Pakhtunkhwa Finance Department's Parents Teachers Councils (PTC)

A hacker claims to have leaked sensitive PTC data from the Finance Department of Khyber Pakhtunkhwa. The breach includes EMIS codes, school and monitor details, account information, and financial data, potentially exposing individuals to identity theft and fraud. The attacker suggests internal system access from September 2024.

This alleged leak draws attention to a critical issue beyond just the exposed data—it highlights the persistent vulnerability in the education sector: insider access. Employees and even students can access school systems, often leading to deeper access into sensitive areas. This type of internal risk continues to be a significant challenge for educational institutions, where monitoring and controlling access can be more difficult, exacerbating security concerns in an already vulnerable sector.



The post in the hacker forum, not every attack on Education targets the schools

#### 4. Fog Ransomware Targets US Education via VPN Access

According to a [research](#), The Fog ransomware group has focused on the US education sector this year, exploiting vulnerabilities in Virtual Private Networks (VPNs). These attacks have disrupted institutions by [encrypting](#) vital systems, crippling operations, and restricting access to data. By targeting educational facilities, Fog ransomware has threatened critical administrative functions, demanding significant ransoms that strained the finances of affected organizations. This highlights the increasing risks faced by schools and universities, underscoring the urgent need for stronger cybersecurity to protect sensitive student and staff data. The specific focus on this sector in 2024 reveals its vulnerability to cyber threats.

#### 5. Data Breach at UK, Thousands of Students Affected in Singapore

Not directly to an educational service but a supply chain effect. A significant cyberattack targeted Mobile Guardian, a UK-based **Mobile Device Management (MDM) firm**, with widespread repercussions in the education sector. Hackers gained unauthorized access to the company's systems, leading to the remote wiping of devices used by approximately 13,000 students across 26 secondary schools in Singapore. The Ministry of Education (MOE) confirmed that while no evidence of data theft was found, the attack severely disrupted students' access to essential applications and resources.

# Mobile Guardian Device Management Application to be Removed from Personal Learning Devices

Published Date: 05 August 2024 11:00 AM | [News, Press Releases](#)

On 4 August 2024 late night, the Ministry of Education (MOE) was alerted by schools that some students who use iPads or Chromebooks as personal learning devices were unable to access their applications and information stored in their devices.

*Terminating the use of Mobile Guardian in all students' devices ([Press Release](#))*

In response to the breach, the MOE promptly removed the Mobile Guardian application from affected devices. This incident once more underscored the vulnerabilities present in educational technology systems.

## 6. Unauthorized Access Sales Signals The Further Attack

---

In a recent incident, an education company in the US was targeted by cybercriminals who advertised unauthorized access for sale on a [hacker forum](#) monitored by SOCRadar. This unauthorized access utilizes the VNC protocol and includes details about the company's network, which comprises over 2,200 devices, more than 10 domains, and various storage and virtualization systems. The total asking price for this access was set at \$3,000.



**Access US**  
 , 3 minutes ago in [Access] - FTP, shells, root, sql-inj, DB, Servers

Posted 3 minutes ago

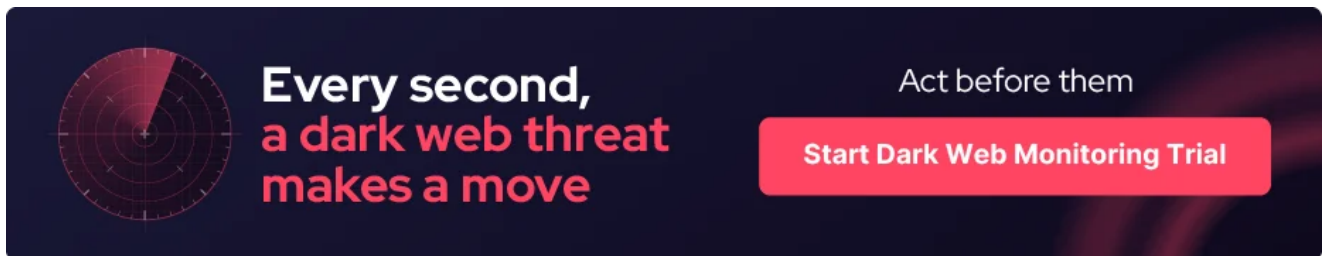
Selling access  
 Country USA  
 Access type: VNC Protocol  
 Activity: Education  
 Network hosts 2208 pcs., domains 10+ pcs.  
 ESXi - 26 pcs.  
 NAS - 3 pcs.  
 Disk Station - 10 pcs.  
 PC is behind the domain, there is Cisco VPN / Global Protect no credits!  
 Zoominfo - \$2.9 Billion  
 OS - Windows AV WinDef

Price: 3k\$

The access sale in a hacker forum

As we discussed in a previous [blog](#), these access sales often lead to sensitive data leaks and ransomware attacks. The education sector continues to face significant cybersecurity threats, with this incident highlighting vulnerabilities that make institutions attractive targets for cybercriminals. Access is being sold with little indication of any security credentials, indicating a troubling level of exploitation in educational settings.

Be sure to check out our blog post, "[The Rise of Initial Access Brokers on the Dark Web](#)," for insights into the potential impacts and trends of access sales.



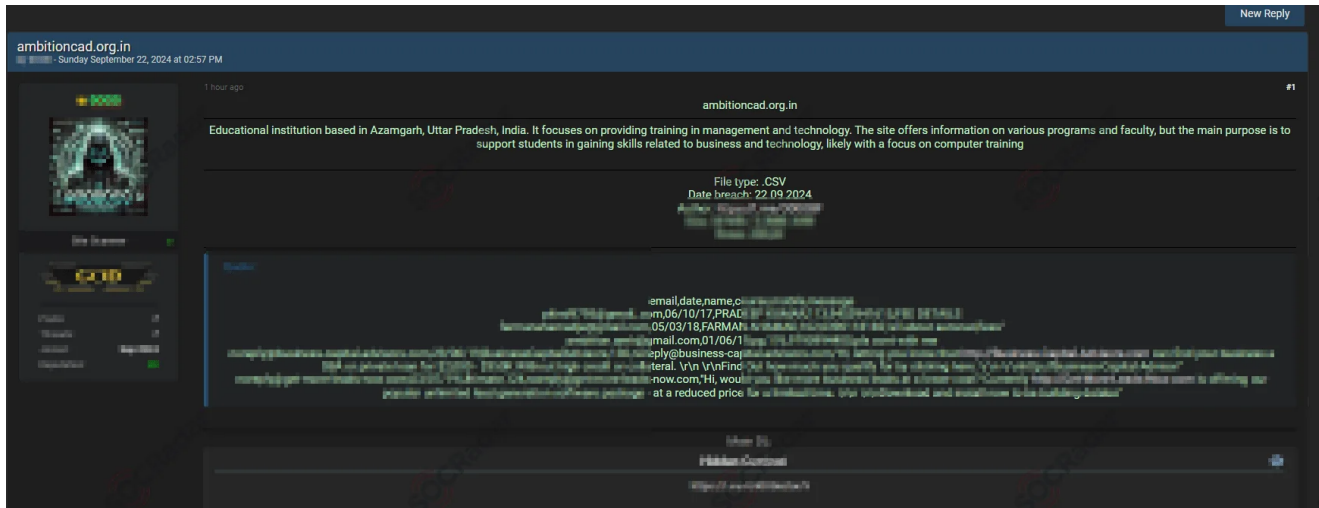
Every second, a dark web threat makes a move

Act before them

Start Dark Web Monitoring Trial

## 7. Not Just Hacktivism, Alleged Database Leak of Ambition Institute of Management & Technology in India

In September 2024, a significant data breach allegedly involving the Ambition Institute of Management & Technology, located in Azamgarh, Uttar Pradesh, India, was detected on a dark web forum. The leaked database is said to contain personal and academic information of both students and faculty, putting them at risk of identity theft, [phishing](#) attempts, and other malicious activities.



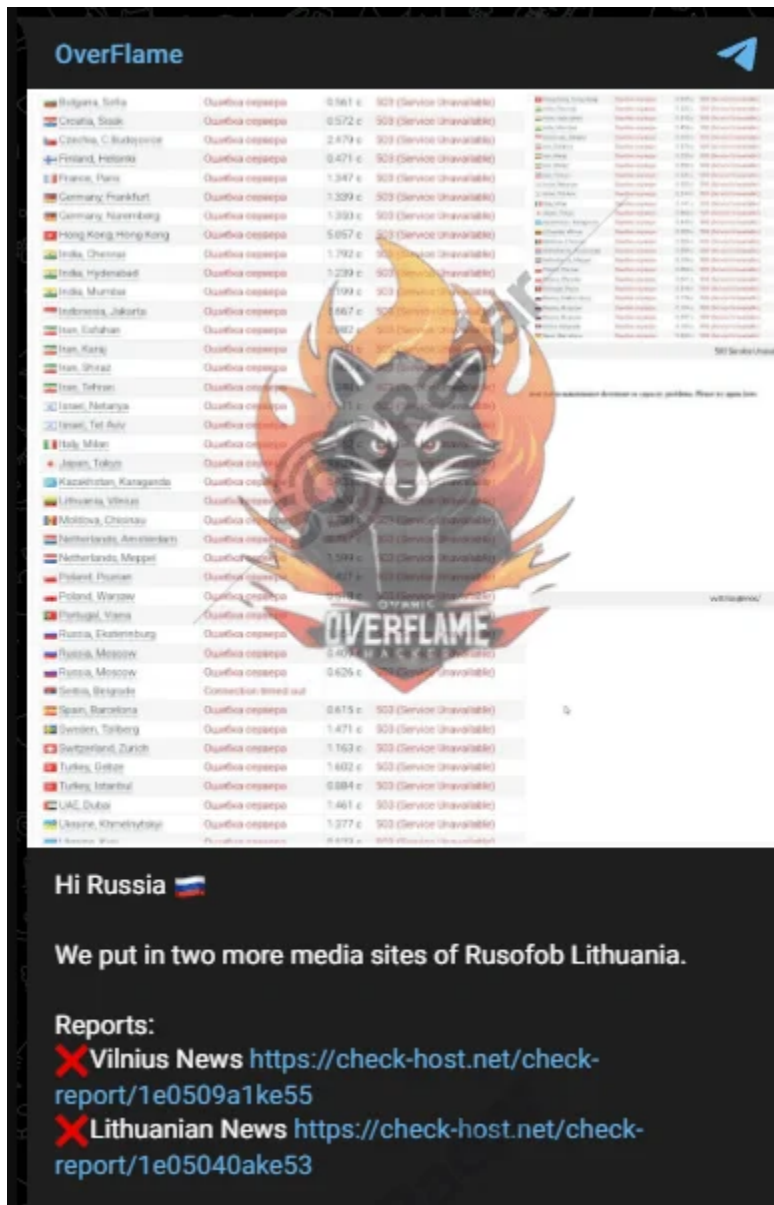
India education industry data for sale in a hacker forum

The breach brings attention to the educational institutions' data protection practices. Furthermore, the availability of this data on hacker forums is a clear indication that threat actors targeting India are not limited to hacktivists, but also include cybercriminals with broader motives.

## 8. A Target For Pro-Russian Threat Actors

The OverFlame group carried out Distributed Denial of Service (DDoS) attacks against Vilnius Vandeny's, a Lithuanian water utility, and Vilnius Lazdynų Mokykla, a local school. The group, known for targeting various Lithuanian institutions, announced the attacks through its Telegram channel. The disruption affected the operations of both institutions, with a potential political or ideological motive behind the choice of targets. OverFlame's use of Telegram for announcing and documenting their attacks demonstrates the increasing role of social platforms in cybercrime communication and coordination.

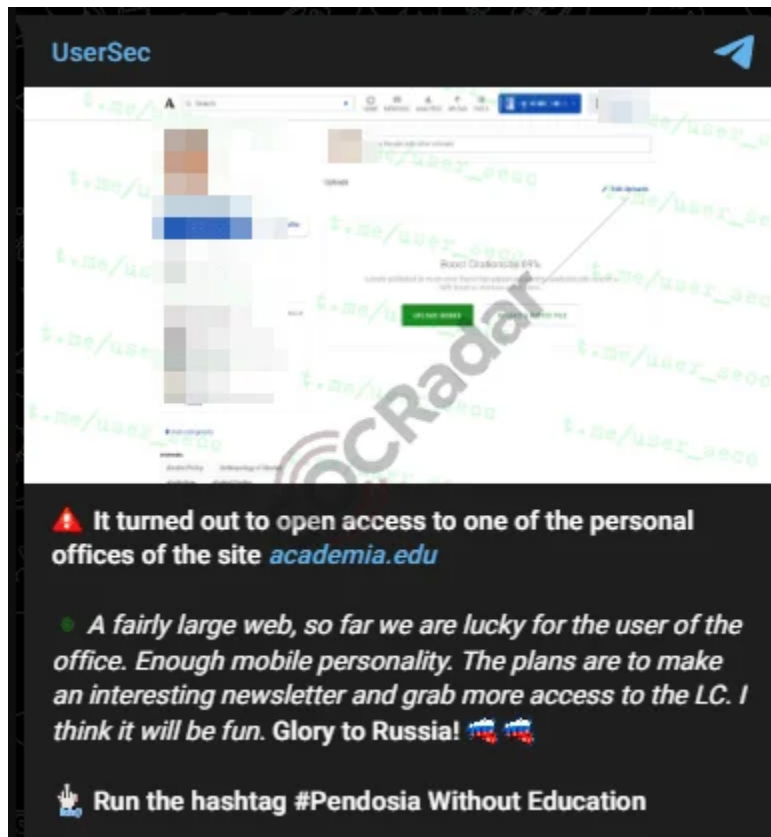
Although the impact and target were not particularly significant, this incident clearly demonstrates how geopolitical events affect various industries, with education often bearing the brunt due to previously highlighted vulnerabilities. The Russia-Ukraine war, in particular, is mirrored on the dark web, where both large and small Russian actors frequently target educational institutions. In this case, it was only a DDoS attack, but given the sensitivity of the data, education can also be a target for espionage by more dangerous threat actors like APT groups. Thus, it's also important to remember that even a brief DDoS attack can serve as a cover for more malicious activities.



A Telegram message of a pro-Russian threat actor, DDoS is a common attack vector for hacktivist groups

## 9. UserSec Launches Cyber Attack on Academia.edu

On September 2, 2024, UserSec, a well-known hacktivist group, executed a cyberattack on Academia.edu, a platform that facilitates academic sharing and networking among researchers. The group announced the attack via their Telegram channel, claiming they had accessed a personal office within the site. This unauthorized access could potentially be exploited for more extensive attacks.



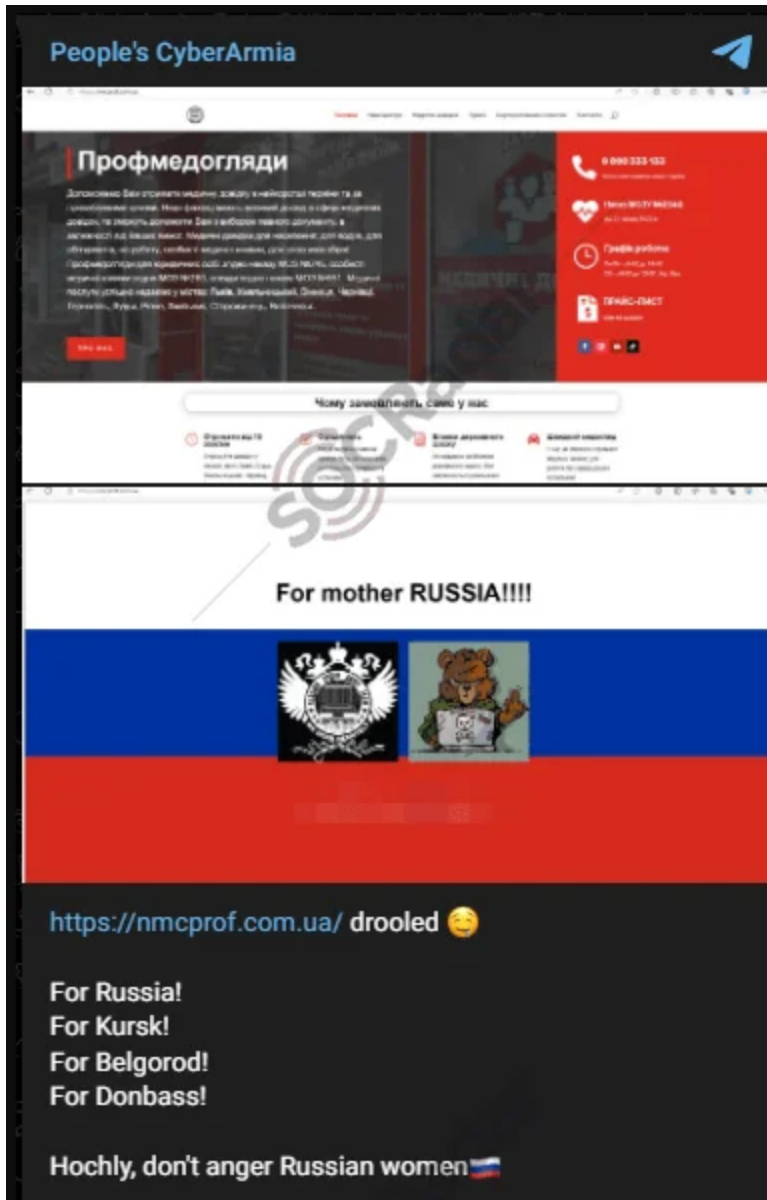
UserSec's Telegram post

UserSec indicated plans to further leverage the compromised account for malicious purposes, hinting at future newsletters or additional unauthorized access. Their message included a provocative geopolitical statement, “#Pendosia Without Education,” suggesting political motivations behind the breach.

This incident raises concerns about data security within educational platforms, particularly regarding sensitive academic research and personal information. With UserSec's ability to infiltrate such an influential site, there is a heightened risk of future exploitation or leaks targeting researchers and educational institutions globally.

## 10. Cyber Army Targets Ukrainian Medical Exams

On August 20, 2024, the pro-Russian hacker group CyberArmy launched a cyberattack on Professional Medical Examinations (PME), a Ukrainian institution that provides certification exams for the healthcare industry. The attack, announced on CyberArmy's Telegram channel, was accompanied by nationalist rhetoric supporting Russia's ongoing military operations in Ukraine.



*Cyber Army of Russia's Telegram post*

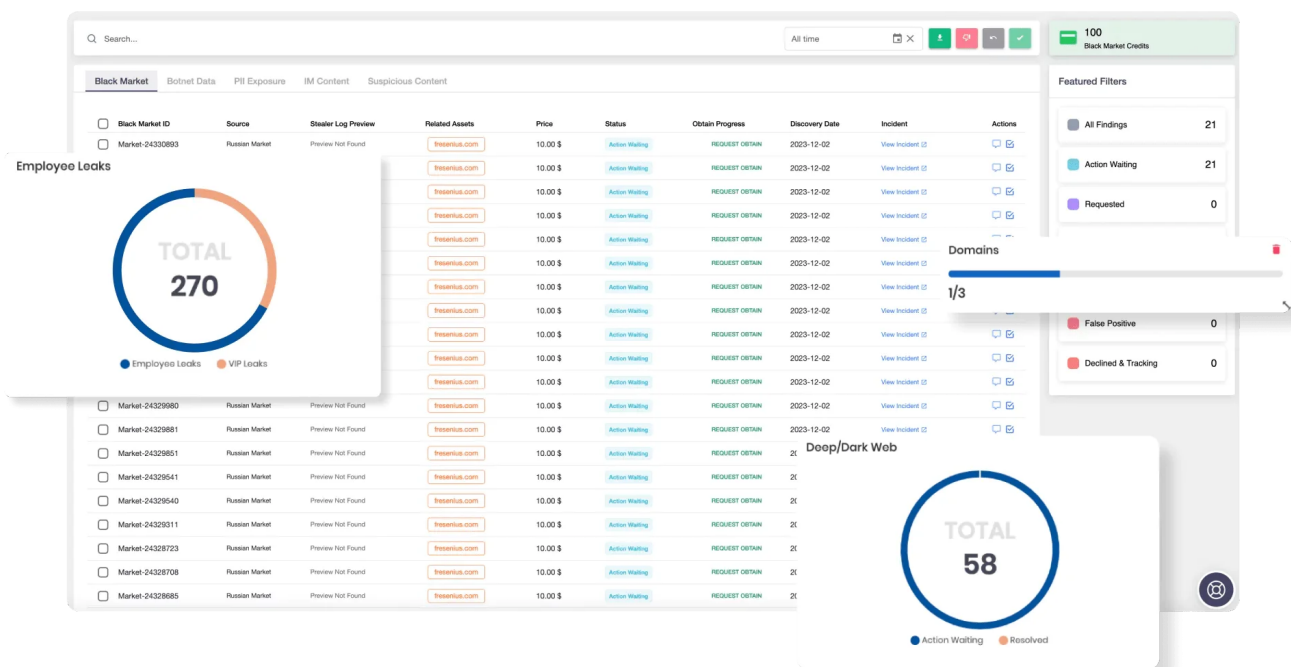
This attack is particularly significant because PME plays a critical role in certifying medical professionals, which is essential for maintaining the healthcare workforce. By targeting an educational center in the healthcare sector, CyberArmy is endangering the examination processes necessary for healthcare workers to qualify and continue their careers. This disruption not only affects healthcare institutions but also risks exposing sensitive medical data, potentially leading to broader complications in the already strained Ukrainian healthcare system. The political motivations behind the attack further highlight the increased cyber risks Ukrainian organizations face amidst the ongoing conflict.

## Conclusion

---

The expanding use of online learning platforms and digital tools has opened up numerous attack vectors for cybercriminals, who often see schools as vulnerable targets due to limited cybersecurity budgets and a reliance on older IT infrastructures. This evolving threat landscape highlights the urgent need for improved cybersecurity measures across the education sector to safeguard against growing attacks. As demonstrated by the diverse range of incidents throughout 2024, from ransomware attacks to data breaches, the education sector is facing unprecedented challenges that require immediate attention and action.

Threat actors, often active on the Dark Web and hacker forums, continue to adapt their tactics. This dynamic environment makes it crucial for educational institutions to implement effective cybersecurity strategies. Solutions offered by SOCRadar provide real-time threat detection and prevention, empowering schools and universities to protect their sensitive data and maintain operational resilience. By prioritizing cybersecurity, educational institutions can not only defend against current threats but also build a robust foundation for a safer digital learning environment in the future.



### SOCRadar's Advanced Dark Web Monitoring: Your Digital Periscope

SOCRadar's Advanced Dark Web Monitoring solution plays a pivotal role in fortifying the cybersecurity posture of educational institutions. By continuously scanning the Dark Web, black markets, and underground forums, SOCRadar helps identify potential threats, such as compromised credentials and leaked sensitive information, before they can be exploited. This proactive approach empowers schools and universities to detect emerging risks early, enabling them to respond swiftly and protect both their data and students' privacy, ensuring a secure learning environment.



**Be Notified Instantly  
When Hackers Mention  
You on Telegram**

*Login to your account and  
configure your alarms*

**→ Login to SOCRadar**

## **PROTECTION OF PERSONAL DATA COOKIE POLICY FOR THE INTERNET SITE**

Protecting your personal data is one of the core principles of our organization, SOCRadar, which operates the internet site ([www.socradar.com](http://www.socradar.com)). This Cookie Usage Policy (“Policy”) explains the types of cookies used and the conditions under which they are used to all website visitors and users.

Cookies are small text files stored on your computer or mobile device by the websites you visit.

Cookies are commonly used to provide you with a personalized experience while using a website, enhance the services offered, and improve your overall browsing experience, contributing to ease of use while navigating a website. If you prefer not to use cookies, you can delete or block them through your browser settings. However, please be aware that this may affect your usage of our website. Unless you change your cookie settings in your browser, we will assume that you accept the use of cookies on this site.

### **1. WHAT KIND OF DATA IS PROCESSED IN COOKIES?**

Cookies on websites collect data related to your browsing and usage preferences on the device you use to visit the site, depending on their type. This data includes information about the pages you access, the services and products you explore, your preferred language choice, and other preferences.

### **2. WHAT ARE COOKIES AND WHAT ARE THEIR PURPOSES?**

Cookies are small text files stored on your device or web server by the websites you visit through your browsers. These small text files, containing your preferred language and other settings, help us remember your preferences on your next visit and assist us in making improvements to our services to enhance your experience on the site. This way, you can have a better and more personalized user experience on your next visit.

The main purposes of using cookies on our Internet Site are as follows:

- Improve the functionality and performance of the website to enhance the services provided to you,
- Enhance and introduce new features to the Internet Site and customize the provided features based on your preferences,

- Ensure legal and commercial security for the Internet Site, yourself, and the Organization, and prevent fraudulent transactions through the Site,
- Fulfill legal and contractual obligations, including those arising from Law No. 5651 on the Regulation of Publications on the Internet and the Fight Against Crimes Committed Through These Publications, as well as the Regulation on the Procedures and Principles Regarding the Regulation of Publications on the Internet.

### **3. TYPES OF COOKIES USED ON OUR INTERNET SITE 3.1. Session Cookies**

Session cookies ensure the smooth operation of the internet site during your visit. They are used for purposes such as ensuring the security and continuity of our sites and your visits. Session cookies are temporary cookies and are deleted when you close your browser; they are not permanent.

### **3.2. Persistent Cookies**

These cookies are used to remember your preferences and are stored on your device through browsers. Persistent cookies remain stored on your device even after you close your browser or restart your computer. These cookies are stored in your browser's subfolders until deleted from your browser's settings. Some types of persistent cookies can be used to provide personalized recommendations based on your usage purposes.

With persistent cookies, when you revisit our website with the same device, the website checks if a cookie created by our website exists on your device. If so, it is understood that you have visited the site before, and the content to be presented to you is determined accordingly, offering you a better service.

### **3.3. Mandatory/Technical Cookies**

Mandatory cookies are essential for the proper functioning of the visited internet site. The purpose of these cookies is to provide necessary services by ensuring the operation of the site. For example, they allow access to secure sections of the internet site, use of its features, and navigation.

### **3.4. Analytical Cookies**

These cookies gather information about how the website is used, the frequency and number of visits, and show how visitors navigate to the site. The purpose of using these cookies is to improve the operation of the site, increase its performance, and determine general trend directions. They do not contain data that can identify visitors. For example, they show the number of error messages displayed or the most visited pages.

### **3.5. Functional Cookies**



Functional cookies remember the choices made by visitors within the site and recall them during the next visit. The purpose of these cookies is to provide ease of use to visitors. For example, they prevent the need to re-enter the user's password on each page visited by the site user.

### **3.6. Targeting/Advertising Cookies**

They measure the effectiveness of advertisements shown to visitors and calculate how many times ads are displayed. The purpose of these cookies is to present personalized advertisements to visitors based on their interests.

Similarly, they determine the specific interests of visitors' navigation and present appropriate content. For example, they prevent the same advertisement from being shown again to the visitor in a short period.

## **4. HOW TO MANAGE COOKIE PREFERENCES?**

To change your preferences regarding the use of cookies, block or delete cookies, you only need to change your browser settings.

Many browsers offer options to accept or reject cookies, only accept certain types of cookies, or receive notifications from the browser when a website requests to store cookies on your device.

Also, it is possible to delete previously saved cookies from your browser.

If you disable or reject cookies, you may need to manually adjust some preferences, and certain features and services on the website may not work properly as we will not be able to recognize and associate with your account. You can change your browser settings by clicking on the relevant link from the table below.

## **5. EFFECTIVE DATE OF THE INTERNET SITE PRIVACY POLICY**

The Internet Site Privacy Policy is dated The effective date of the Policy will be updated if the entire Policy or specific sections are renewed. The Privacy Policy is published on the Organization's website ([www.socradar.com](http://www.socradar.com)) and made accessible to relevant individuals upon request.

SOCRadar

Address: 651 N Broad St, Suite 205 Middletown, DE 19709 USA

Phone: +1 (571) 249-4598

Email: [\[email protected\]](#)

Website: [www.socradar.com](http://www.socradar.com)