DATASHEET

GUARDIANS OF KNOWLEDGE

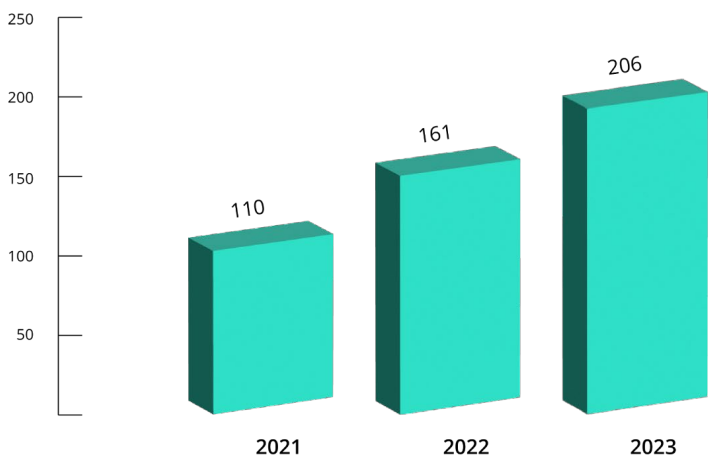
SAFEGUARDING EDUCATION INSTITUTIONS AGAINST CYBERCRIME THREATS

The education sector remains one of the most targeted sectors by cybercriminals in 2023. Although the COVID-19 pandemic is no longer a current concern and remote learning is less widespread than before, educational institutions continue to be soft targets for cybercriminals. In August 2023, the Biden administration launched new efforts to strengthen America's K-12 Schools' cybersecurity. With the beginning of the new school year, KELA delves deep into the persistent threats against the education sector including ransomware attacks, network access offers, hacktivist groups' attacks, and data breaches.

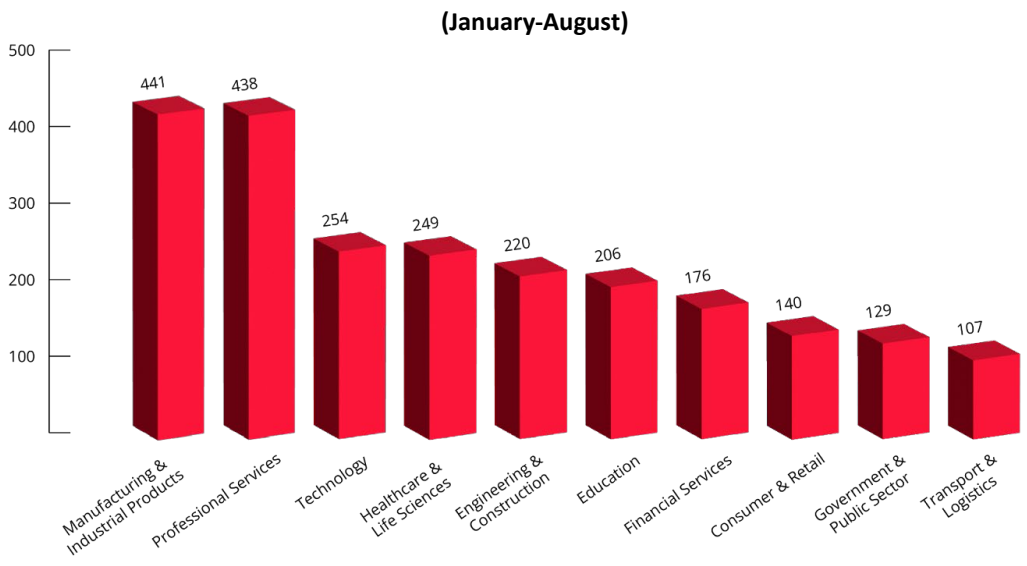
RANSOMWARE ATTACKS

KELA's analysis of ransomware victims and data leak activity shows that ransomware and extortion actors remained a highly persistent threat, **impacting over 470 victims** since 2021. In 2023 so far, the education sector is in the top 6 most targeted sectors with more than 200 attacks. The **most targeted country is the US**, with 310 attacks during the last three years, accounting for almost 60% of the ransomware attacks in this sector. Other top targeted countries are the **UK, Canada, Australia** and **Spain**.

Ransomware attacks against the education sector (January-August 2023)



Top targeted sectors in 2023 (January-August)

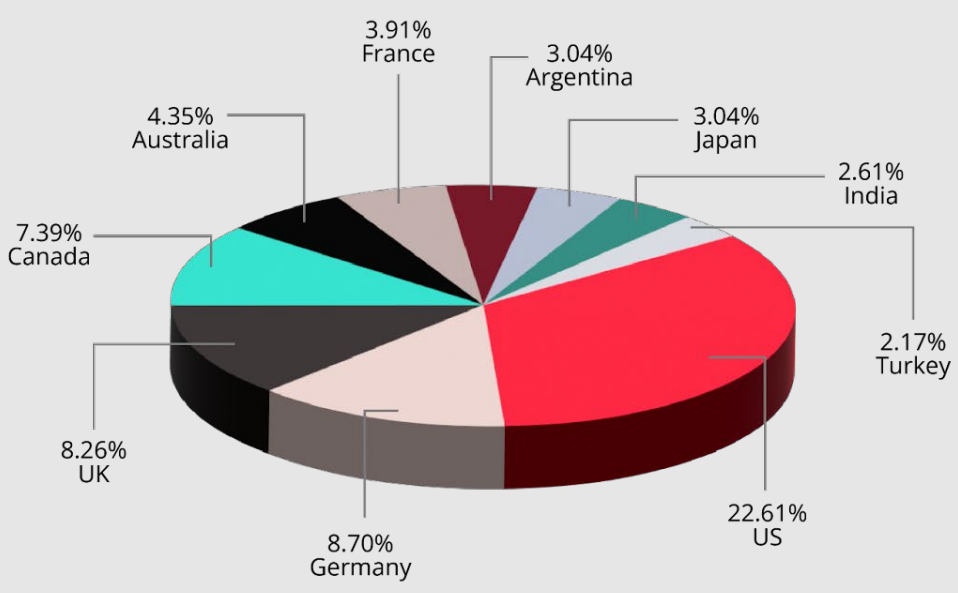


The most prolific ransomware groups targeting the education sector were **LockBit, Vice Society and Clop**, which were responsible for 30% of the ransomware attacks over the last three years. Vice Society is a notorious ransomware group known for targeting the education sector, K-12 and higher education institutions in particular.

NETWORK ACCESS OFFERS

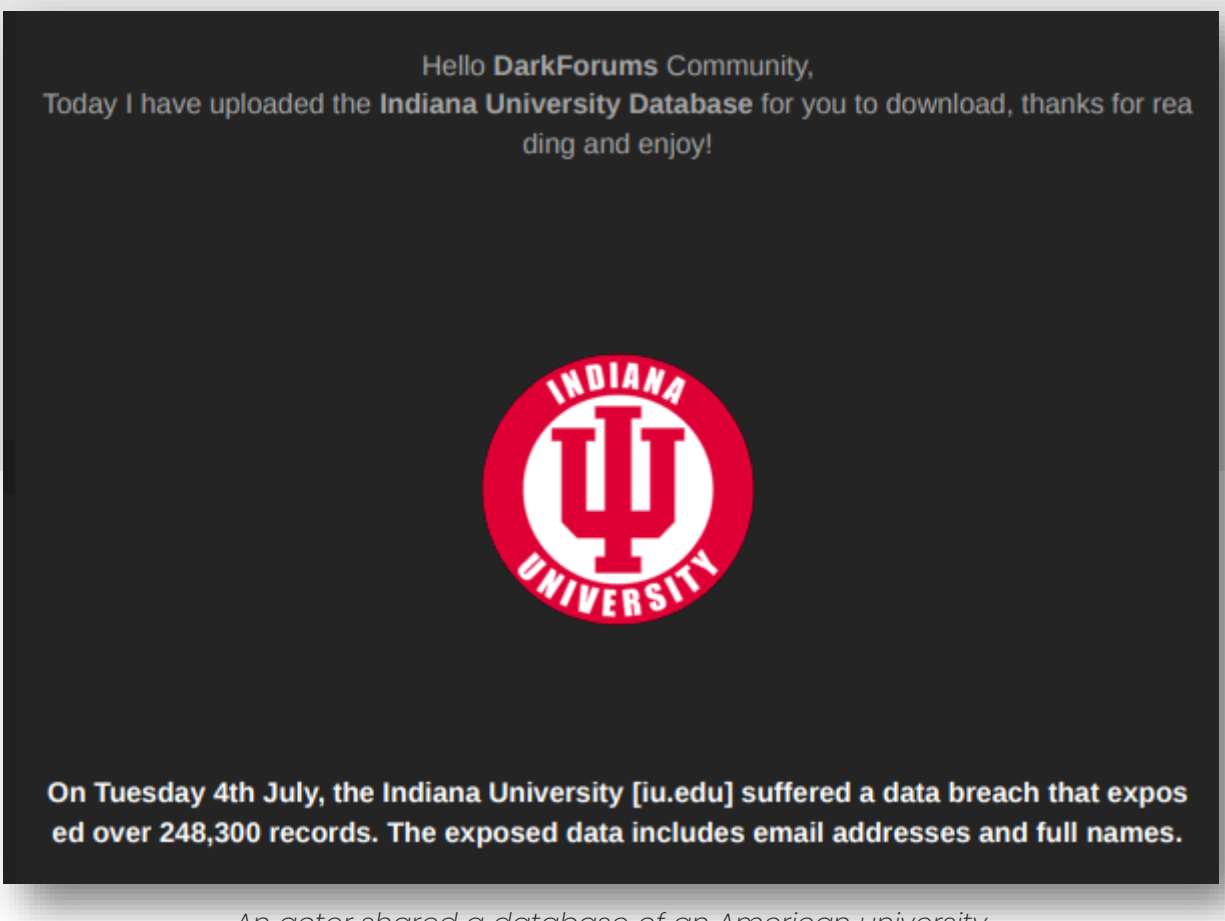
Initial Access Brokers (IABs) play an important role in a ransomware-as-a-service supply chain by supplying access to compromised networks. A large number of people, including students and staff, access systems and networks, many from home or outside the network, which makes the education sector much more vulnerable to such attacks. KELA identified around 230 network access listings to companies from the education sector for sale between 2021 to 2023. **The US was the most targeted country by IABs**, accounting for 22% of the victims, followed by **Germany, UK, Canada, and Australia**.

Top targeted countries in the education sector by IABs (January-August 2023)



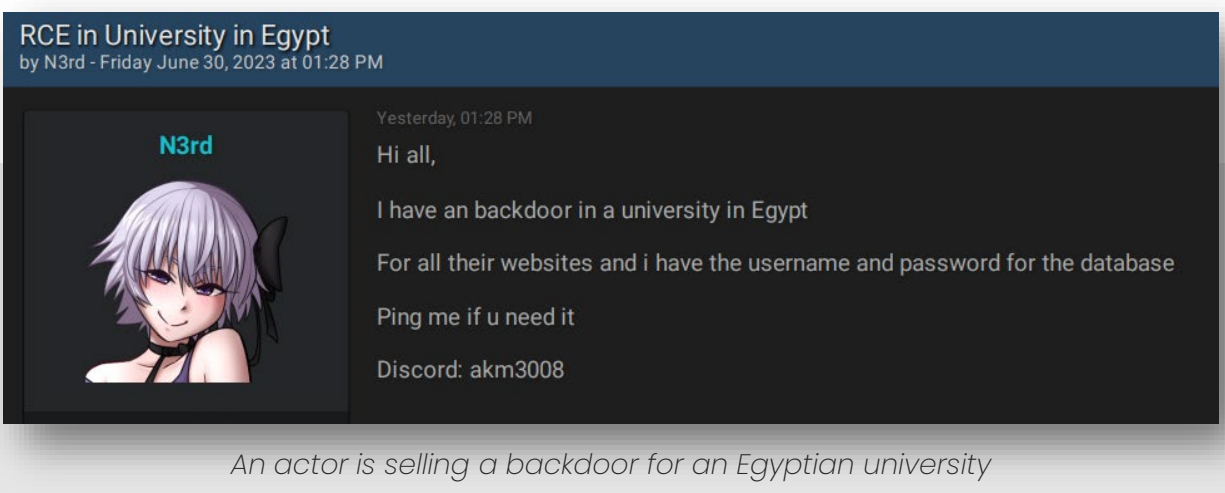
DATABASE DUMPS

Education institutions possess sensitive information that can be attractive to cybercriminals. KELA observed leaks and sales of educational entities' data PII (Personal Identifying Information), including students' names, email addresses, physical addresses, phone numbers, etc. In July 2023, an actor shared a database of Indiana University allegedly exposing over 248,300 records, including email addresses and full names.

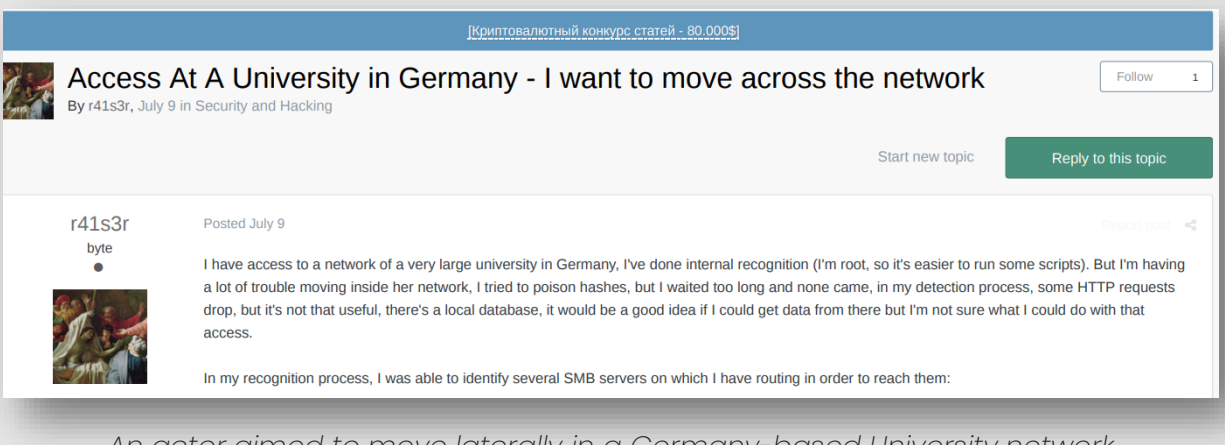


An actor shared a database of an American university

Threat actors also share exploits to exploit web vulnerabilities of educational institutions that enable them to gain unauthorized access to sensitive databases. For example, an actor shared on BreachForums backdoor allows access to the Egypt-based university database.



An actor is selling a backdoor for an Egyptian university



An actor aimed to move laterally in a Germany-based University network

ACCOUNTS COMPROMISED BY INFO-STEALERS

Another method for actors to get access to sensitive information of educational entities is to acquire bots from botnet markets such as Russian Market, Genesis, and TwoEasy (enabling the individual purchase of bots), and Telegram channels, also known as "clouds of logs". After acquiring login credentials, threat actors utilize these valuable assets in various campaigns, ranging from phishing to ransomware attacks. KELA's analysis of Russian Market compromised accounts shows that among the top 15 targeted services of educational institutions, that were infected by info-stealing malware, almost 70% belong to US universities, among them top US universities.

RECOMMENDATIONS AND MITIGATIONS

•**Security awareness training:** Educate staff, students, and parents about the basics of cybersecurity, including identifying phishing emails, strong password practices, and safe online behavior.

•**Regular backups:** Maintain regular backups of critical data and systems and store them securely offline to mitigate the impact of ransomware attacks.

•**Multi-Factor Authentication (MFA):** Implement MFA for accessing sensitive data and systems to add an extra layer of security, making it challenging for threat actors to reuse credentials.

Monitor cybercrime platforms: monitor cybercrime sources to identify cybercrime chatter about database dumps, compromised accounts, cyber trends and ransomware attacks. **Get started with KELA for free today!**