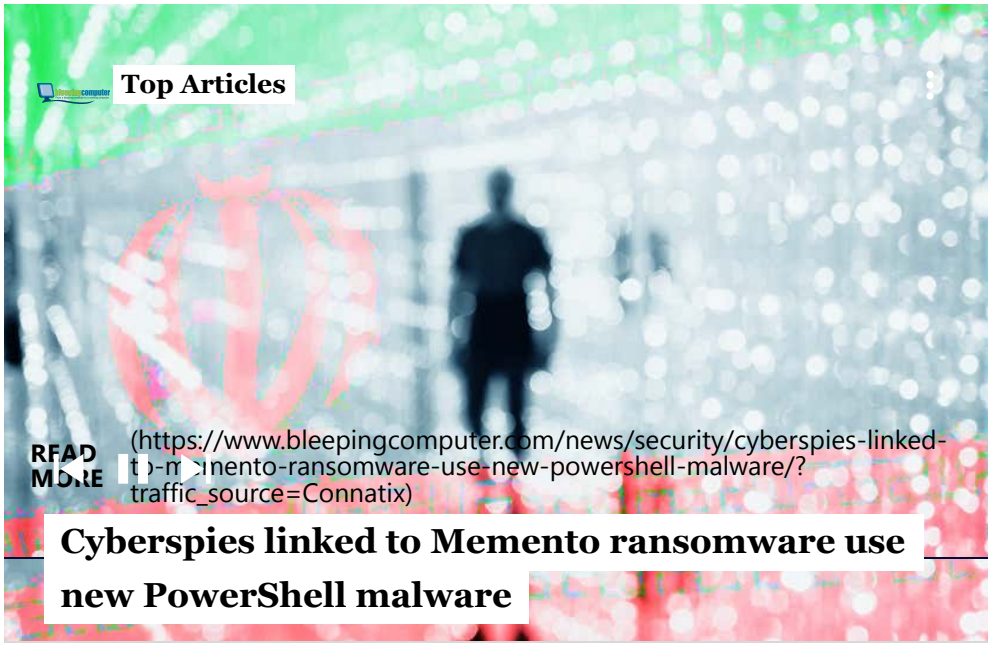
British Council exposed more than 100,000 files with student records

By **Ax Sharma (https://www.bleepingcomputer.com/author/ax-sharma/)** February 1, 2022 08:24 AM 0

More than 100,000 files with student records belonging to British Council were found exposed online.

An unsecured Microsoft Azure blob discovered on the internet by a cybersecurity firm revealed student names, IDs, usernames and email addresses, and other personal information.

British Council promotes the study of British culture and the English language around the world and is known for administering the IELTS standardized language exam.



Unsecured Azure blob spills Excel, XML, JSON files

British Council, the global organization for promoting British culture, the English language, and education opportunities, was leaking over 144,000 files containing student records.

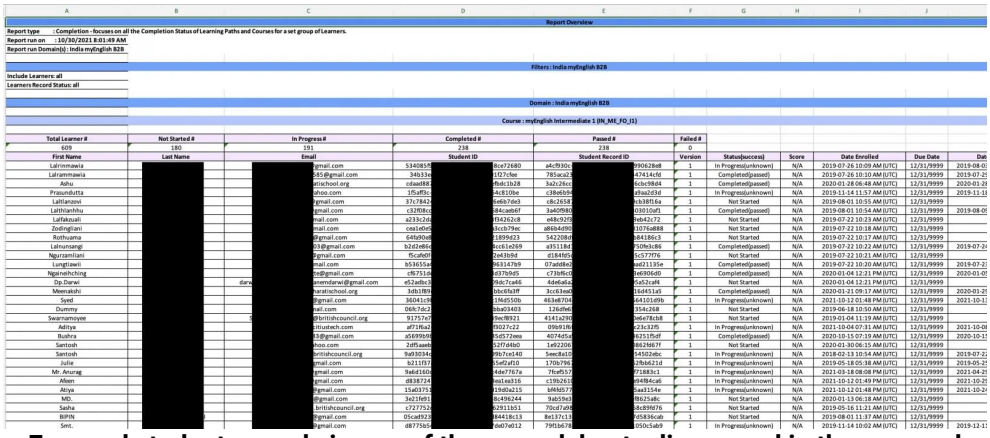
Cyber security firm Clario, along with security researcher Bob Diachenko discovered the leak in December 2021 and immediately reported their findings to British Council.

Spread across more than 100 countries, British Council has previously been dubbed the 'soft power (https://www.newstatesman.com/culture/2021/07/Robert-winder-soft-power-great-game-review)' arm of the UK foreign policy. Although partially funded by the UK Government via a grant, the independently operated non-profit generates the vast majority of its revenue from activities like teaching, exams, tendered contracts, and partnerships.

The organization also administers the International English Language Testing System (IELTS) exam, the most recognized standardized English language test around the world, alongside TOEFL (https://en.wikipedia.org/wiki/Test_of_English_as_a_Foreign_Language).

According to the researchers, an unprotected Azure blob container was indexed by a public search engine and contained thousands of Excel spreadsheets and XML/JSON files, viewable by anyone.

These files had the personal information of hundreds of thousands of British Council English course learners and students from around the world.



Exposed student records in one of the spreadsheets discovered in the exposed Azure blob (Clario)

The exposed information included:

- Full name
- Email address
- Student ID
- Student status
- Enrollment dates
- Duration of study
- Notes

It isn't known for how long was this data available online to the public, with no authentication in place, state the researchers.

Another example of an XML file with personal information is shown below:

XML files exposing student records

British Council: 10,000 records held by third-party provider

Diachenko and Clario discovered the data leak on December 5th, 2021, and promptly notified British Council.

One of the main concerns the researchers had at the time was the risk from phishing actors and identity thieves—should they get their hands on this information.

After not hearing back for 48 hours from British Council, the researchers reattempted contact; this time via Twitter, which is where subsequent communication between the two parties took place.

"On December 23rd, 2021 (two weeks after the initial contact), confirmation around the security of the repository was announced," state the researchers.

BleepingComputer also reached out to British Council to independently confirm the information and we were provided with the following statement:

> "The data in question was held and processed by a third party service provider. Approximately 10,000 records were accessible in a way that should not have occurred. On becoming aware of this, our third party service provider immediately secured the records with appropriate controls and the data in question was rendered no longer accessible.

> We are working with the supplier to ensure similar incidents do not happen in the future.
>
> We have reported the incident in accordance with our regulatory obligations and we remain in contact with the Information Commissioner's Office should any further action be required.
>
> The British Council takes its responsibilities under the Data Protection Act 2018 and General Data Protection Regulations (GDPR) very seriously. The privacy and security of personal information is paramount," a British Council spokesperson told BleepingComputer.

As noted, although the researchers discovered over 144,000 files, according to British Council, just about 10,000 student records were affected.

The disclosure of this data leak follows a last month's report (https://www.infosecurity-magazine.com/news/british-council-ransomware-attacks/) stating British Council had been a victim of "two successful ransomware attacks over the past five years," in addition to six unsuccessful attempts by ransomware ops.

As a result of these attacks, British Council had reportedly experienced 12 days of downtime in total—five days in the first case, and seven in the second. However, the organization didn't pay a ransom either time.

Given the prominent place held by the British Council in promoting UK culture abroad, and its role in co-managing the IELTS exam, it isn't hard to see why threat actors would be lured to target the institution.

Clario recommends British Council students and test-takers to keep an eye out for any suspicious phishing emails they may receive, and to change their login passwords immediately as an extra precaution.