Russia-linked cybercriminals target school for children with learning difficulties

By Alexander Martin

Published: 2023-08-02 · Archived: 2026-04-02 10:39:33 UTC

The LockBit ransomware group, potentially the world's most prolific cybercrime organization, is attempting to extort a school for children with special educational needs.

West Oaks School, in Leeds, England, has a capacity for 440 pupils between the ages of 2 and 19. It was listed on the gang's darknet site on July 31 alongside a notice that the school had two weeks to make a ransom payment or the purportedly stolen data would be published.

The school — which is currently on its summer break — specializes in education for children "with a wide range of needs including profound, multiple, and complex conditions, autistic spectrum conditions and severe learning difficulties."

It is not clear what information, if any, was stolen from the school, nor whether its computer network had been encrypted. As is typical, the listing simply claims "all available data will be published."

The day before publication, Recorded Future News emailed the school's generic contact address, and emailed headteacher Andrew Hodkinson, as well as the chair of its governing body, John Hayton, to ask for a statement regarding whether teachers, parents, and regulators had been informed about the incident. These emails, and a message left on the school's phone system, were not answered.

West Oaks is the latest educational establishment in Britain to face a ransomware incident, with a large number of attacks prompting repeated warnings from cyber authorities in recent years.

Britain's National Cyber Security Centre (NCSC) first issued an alert to British schools about ransomware attacks in September 2020 warning of "an increased number of ransomware attacks affecting education establishments in the U.K., including schools, colleges, and universities."

The alert page states that it has been updated several times since then due to further ransomware attacks.

The NCSC continued to reference an increase in attacks earlier this year when it published a survey finding that "despite an increase in the number of ransomware attacks" schools were becoming "better prepared" to deal with these incidents. This preparation includes protecting IT networks but also focusing on a quick recovery from the incident itself.

Asked previously about the number of attacks impacting schools in the United Kingdom, a spokesperson for the Department for Education told The Record the department monitors cybersecurity incidents closely and that there is no evidence to suggest attacks are on the rise.

This year has seen multiple incidents affecting Tanbridge House School in West Sussex, Wymondham College in Norfolk — the largest state boarding school in the country — and Guildford County School in Surrey, where the extortionists appeared to leak safeguarding reports, sensitive internal documents teachers write to record information about at-risk students.

“Cyber-attacks on schools undermine the hard work of school leaders and are completely unacceptable,” said the spokesperson for the Department for Education, adding that they provide a risk protection arrangement to more than 9,500 schools throughout England. The program includes cover for cyber incidents as well as access to a 24/7 incident response service.

LockBit, the gang behind the attack on West Oaks School, was also behind the attack on Royal Mail earlier this year.

The LockBit model

The LockBit brand itself was first observed on Russian-language cybercrime forums in January 2020 and, as of 2022, was responsible for more attacks on U.S. government offices — one in six — than any other group.

A joint cybersecurity advisory on the group circulated in June by authorities in the U.S., United Kingdom, France, Germany, Canada, Australia and New Zealand, described LockBit as the “most deployed ransomware variant across the world.”

The 30-page advisory explains how LockBit “functions as a Ransomware-as-a-Service (RaaS) model where affiliates are recruited to conduct ransomware attacks using LockBit ransomware tools and infrastructure,” with the main gang taking a cut of the affiliates’ earnings.

The gang previously apologized after encrypting the network of Canada’s largest children’s hospital and then offered the hospital the decryptor for free, although even with the decryptor available the incident still delayed patient care.

It was not the first time a ransomware group offered a decryptor to a hospital after an attack. Both the Conti and DoppelPaymer ransomware gangs offered free decryptors following massive attacks on Ireland's healthcare system and Helios University Hospital, respectively.

Even with the decryptor — and after proving that it was found to be viable and effective — the work to recover Ireland’s entire healthcare network was a “significant undertaking,” as explained by its interim chief technology officer, John Ward.

“Despite having the key, it still took us four months to recover 99% of the systems. I couldn't tell you, had we not had that key, how long it would have taken.”

[Alexander Martin]

is the UK Editor for Recorded Future News. He was previously a technology reporter for Sky News and a fellow at the European Cyber Conflict Research Initiative, now Virtual Routes. He can be reached securely using Signal on: AlexanderMartin.79
