ThreatDown™
Powered by Malwarebytes

Ransomware Threat Report

Ransomware in the United Kingdom
April 2022–March 2023

May 2023

ThreatDown
Powered by Malwarebytes

The UK: Just like the USA

In the 12 months from April 2022 to March 2023, the United Kingdom suffered more known ransomware attacks than any country other than the USA. Attacks were directed at organisations of all sizes, but several household names joined the roll call of victims.

In August 2022, a ransomware attack on IT supplier Advanced caused widespread outages across the United Kingdom's National Health Service (NHS), the biggest employer in Europe.

Later that year, a ransomware gang attacked British newspaper The Guardian, which operates one of the most visited websites in the world, in a "highly sophisticated cyberattack."

In January 2023, Britain's multinational postal service, Royal Mail, was attacked by LockBit, which demanded the largest known ransom demand ever: $80 million. Royal Mail rejected the demand, and its attackers published the files stolen from the company on the dark web.

Although the gap between the number of attacks in the United Kingdom and the USA looks very large, the two countries are far closer than they seem when it comes to ransomware.

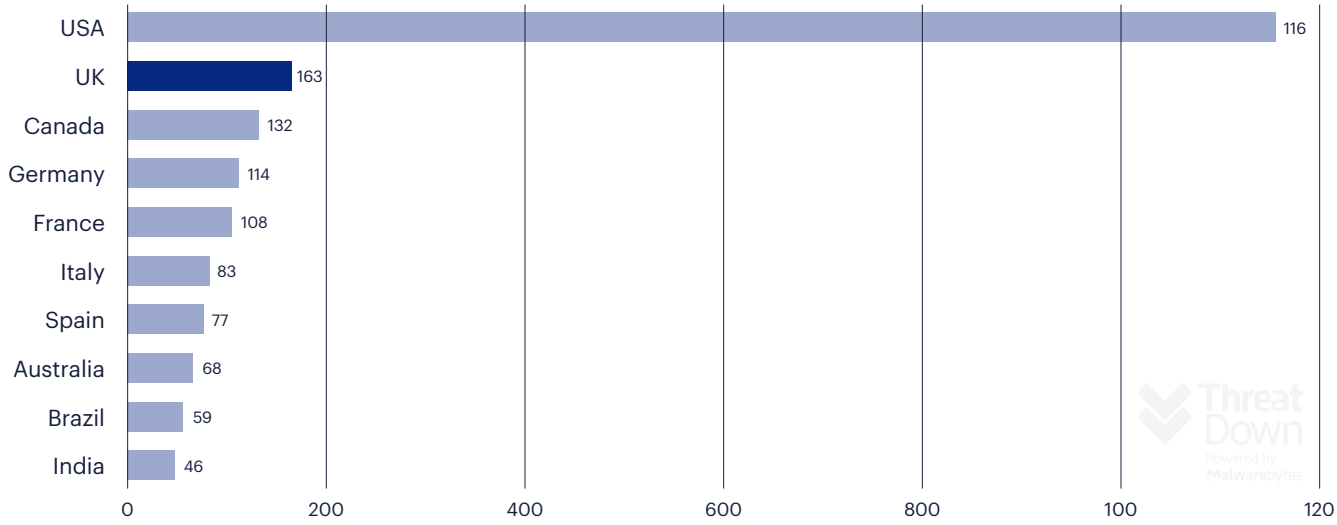
Between April 2022 and March 2023, the UK was:

The second most attacked country in the world

The country with the largest ever ransomware demand

The country where education was targeted far more than any other

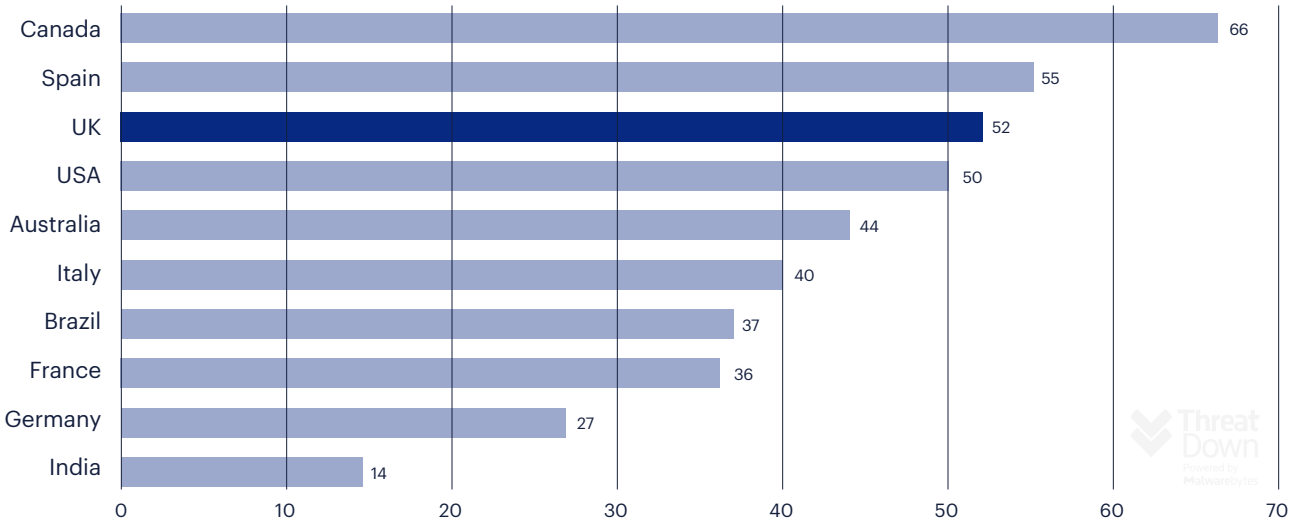
Known attacks in the ten most attacked countries, April 2022 - March 2023



The USA suffered a little over seven times more attacks than the United Kingdom, but its economy, measured by gross domestic product (GDP), was also about seven times larger than the United Kingdom.

Dividing the number of known ransomware attacks by a country's nominal GDP gives us an approximate rate of attacks per $1T of economic output. On that basis, the USA and the United Kingdom are no different and suffered nearly identical rates of attack—around 50 per $1T of GDP.

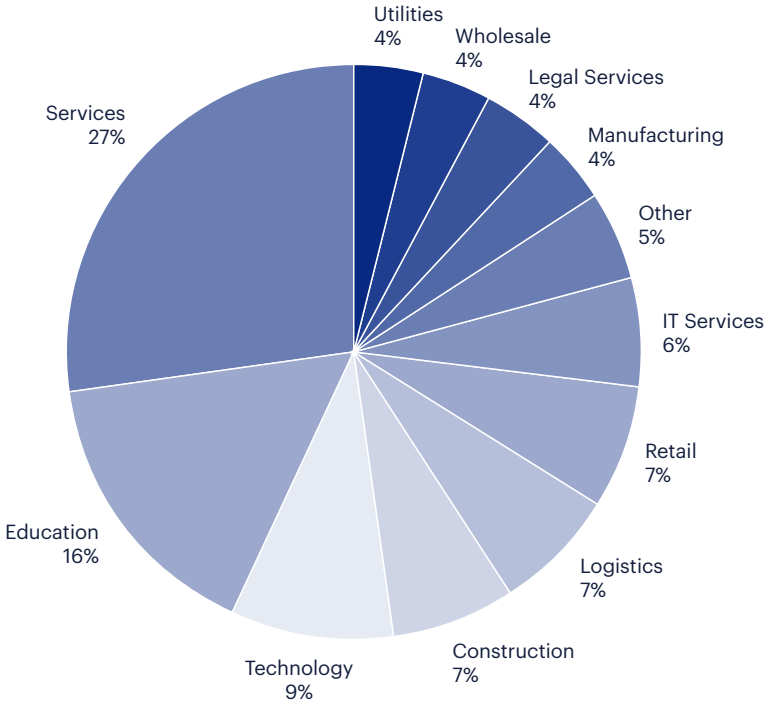
The ten most attacked countries between April 2022 - March 2023, ordered by attacks per $1T GDP



Education, education, education

Over the last 12 months, education was the second most attacked sector in the United Kingdom and suffered far more than in other countries. It was the target in 16% of known attacks in the United Kingdom, but only 4% in France and Germany, and 7% in the USA.

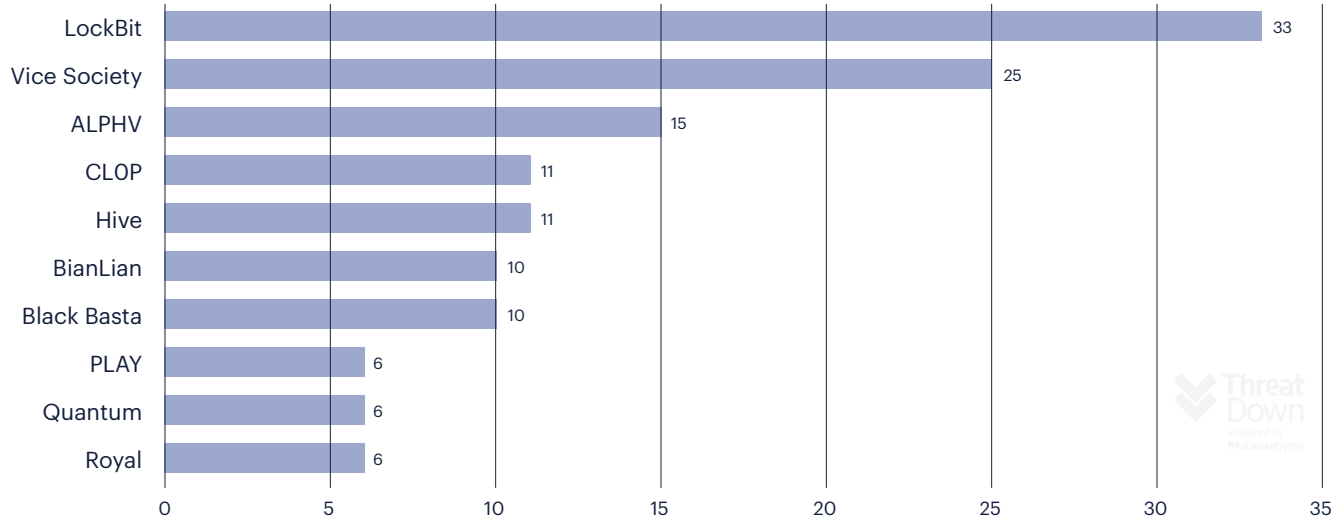
Known ransomware attacks by industry sector in the United Kingdom, April 2022 - March 2023



One of the main reasons for this is Vice Society, an extremely dangerous ransomware group with an appetite for targets in the education sector.

As you'd expect given its global preeminence, LockBit was the most widely used ransomware in the United Kingdom in the last 12 months. However, the gang that occupied second place globally, ALPHV, was knocked into third place in the United Kingdom by Vice Society.

Known attacks by the ten most used ransomware in the United Kingdom, April 2022 - March 2023

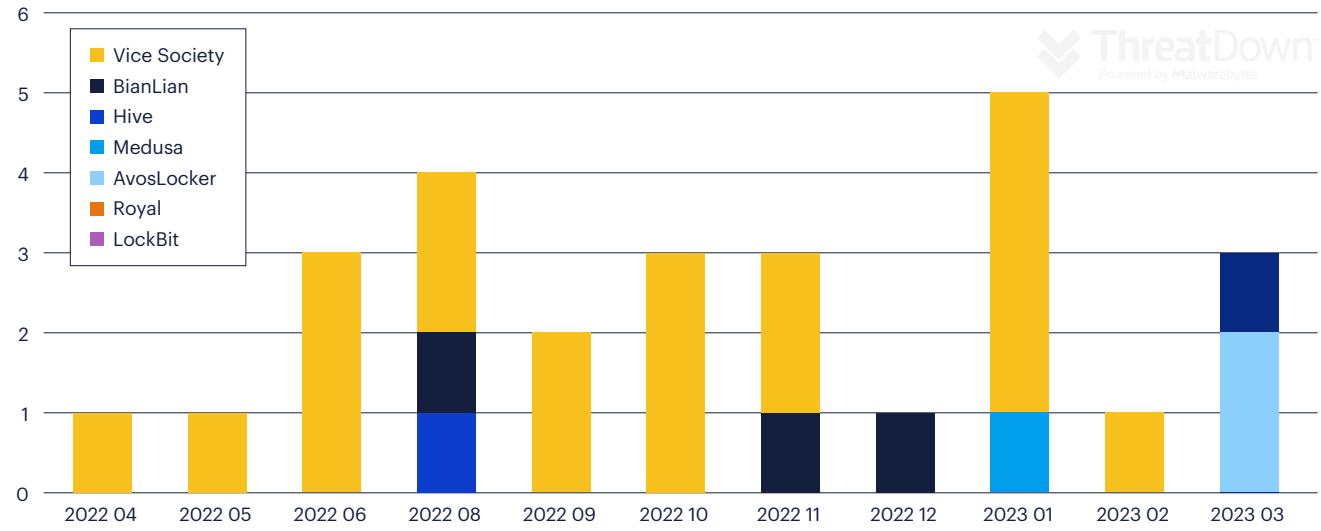


The United Kingdom was one of Vice Society's favourite targets, accounting for 21% of the group's known attacks, just behind the USA's 23%, and far ahead of the next country, Spain, which accounted for 8%.

Sadly, Vice Society's disproportionate interest in the United Kingdom lands squarely on the education sector.

76% of Vice Society's known attacks in the United Kingdom hit the education sector, and Vice Society was responsible for 70% of known attacks on United Kingdom education institutions.

Known ransomware attacks by month on the United Kingdom education sector, by gang, April 2022 - March 2023



It is worth remembering that our numbers only reflect attacks where a ransom wasn't paid, and the true number of attacks is far larger.

In 2023, the BBC reported on 14 schools in the United Kingdom that were attacked by Vice Society including Carmel College, St Helens, Durham Johnston Comprehensive School, and Frances King School of English, London/Dublin.

Vice Society uses familiar techniques such as phishing, compromised credentials, and software exploits to establish a foothold. It is known to practice "living off the land", a technique that allows it to hide in plain sight on a victim's networks, avoiding detection by using the victim's own tools and accounts to prepare their attack. The only effective way to spot attackers who are living off the land is with EDR software operated by experienced security staff, or with a service like MDR.

We can only speculate about why Vice Society has such an appetite for United Kingdom schools, colleges, and universities, but we do know that education in the United Kingdom has suffered a significant drop in funding in the last decade. According to the non-partisan Education Policy Institute, "between 2009–10 and 2019–20, spending per pupil in England fell by 9 percent in real terms."

Following a spike in inflation in 2022, the United Kingdom's largest teaching union voted to strike for better pay for its members, providing further evidence of the deteriorating financial situation in United Kingdom education.

ThreatDown, powered by Malwarebytes, has interviewed several people involved in providing cyber-protection for United Kingdom schools. The picture in each was the same: Cybersecurity was one responsibility among many being carried by very small numbers of IT staff who were under tremendous pressure, and ill-equipped to fight off the attentions of a sophisticated ransomware gang like Vice Society.

Hiring an army of new IT staff is not an option for most schools. For them, the only viable option is cost-effective security software that combines multiple layers of protection and human expertise in an easy-to-use package.

Why ThreatDown, powered by Malwarebytes?

All-in-one endpoint security portfolio that combines 21 layers of protection, threat intelligence, and human expertise in an easy-to-use solution, to secure organizations without requiring an army of IT staff from the latest threats including ransomware, malware, viruses and other attacks.

PREVENT MORE	Pre- and post-execution protection immediately **stops threats at every stage** of the attack cycle.
DETECT EARLIER	AI, ML and signature technologies **detect and interrupt payload delivery** before malicious actions can be performed.
RESPOND FASTER	Human-led investigation coupled with powerful EDR technology **identifies and remediates** advanced and persistent threats.
RECOVER FULLY	Patented Linking Engine **completely removes** all malware traces, artifacts and configuration changes, to prevent ransomware reinfection.

Talk to a threat expert >

ThreatDown Powered by Malwarebytes | www.malwarebytes.com/business | corporate-sales@malwarebytes.com | 1.800.520.2796