ThreatDown™
Powered by Malwarebytes

2023 UK STATE OF RANSOMWARE

State of Ransomware - Summer 2023

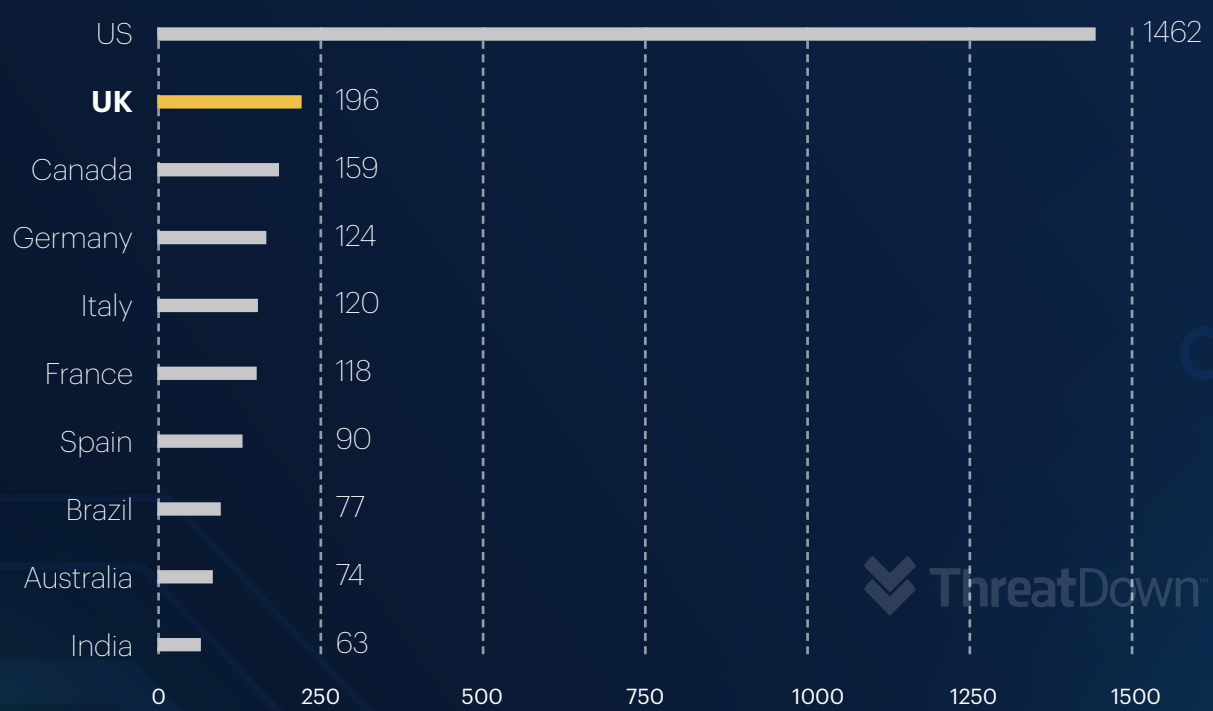
BETWEEN JULY 2022 AND JUNE 2023

- → The UK remains the second most attacked country in the world
- → Attacks on the UK have increased significantly in the last three months
- → The recent success of CLOP may foreshadow a further escalation

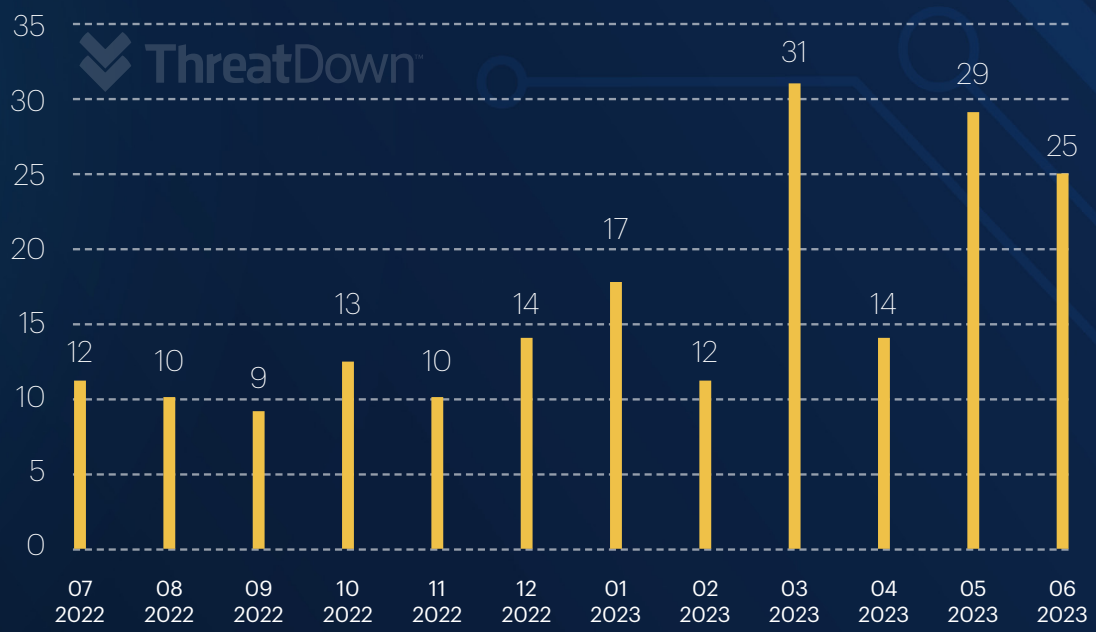
RANSOMWARE IS GETTING WORSE IN THE UK

In the 12 months from July 2022 to June 2023, the UK retained its place as ransomware's second favourite home, suffering more known ransomware attacks than any country other than the US.

Known attacks in the 10 most attacked countries
July 2022 - June 2023

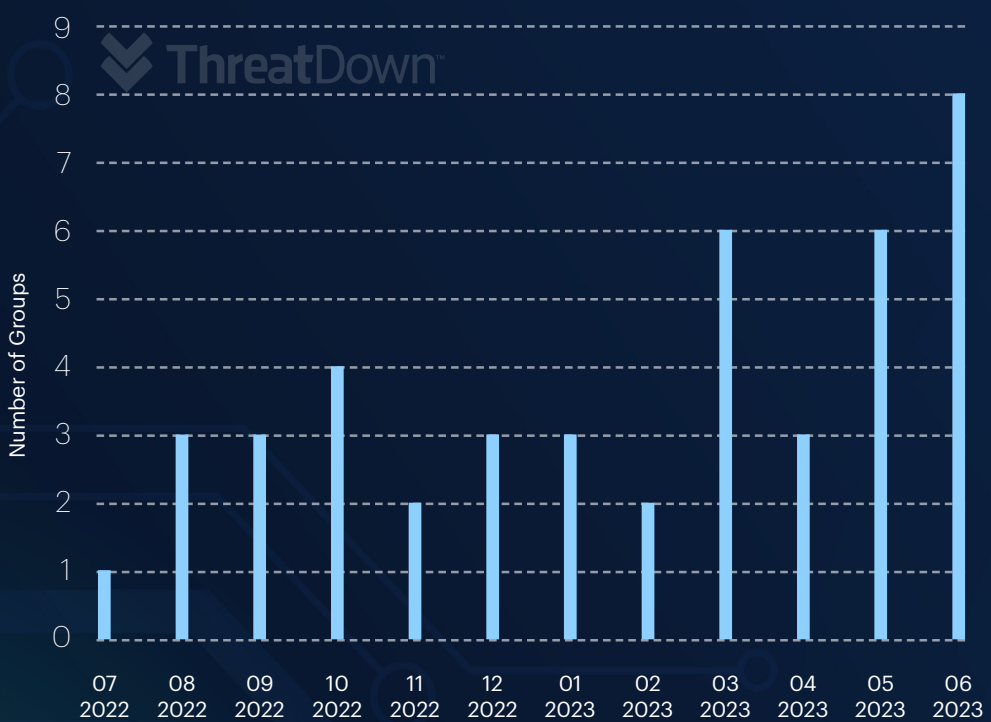


Known attacks in the UK per month
July 2022 - June 2023



Like its large Atlantic neighbour, it has experienced a notable increase in known attacks over the last four months, with March, May, and June all experiencing about double the typical number.

Number of gangs reporting more than one attack per month in the UK
July 2022 - June 2023

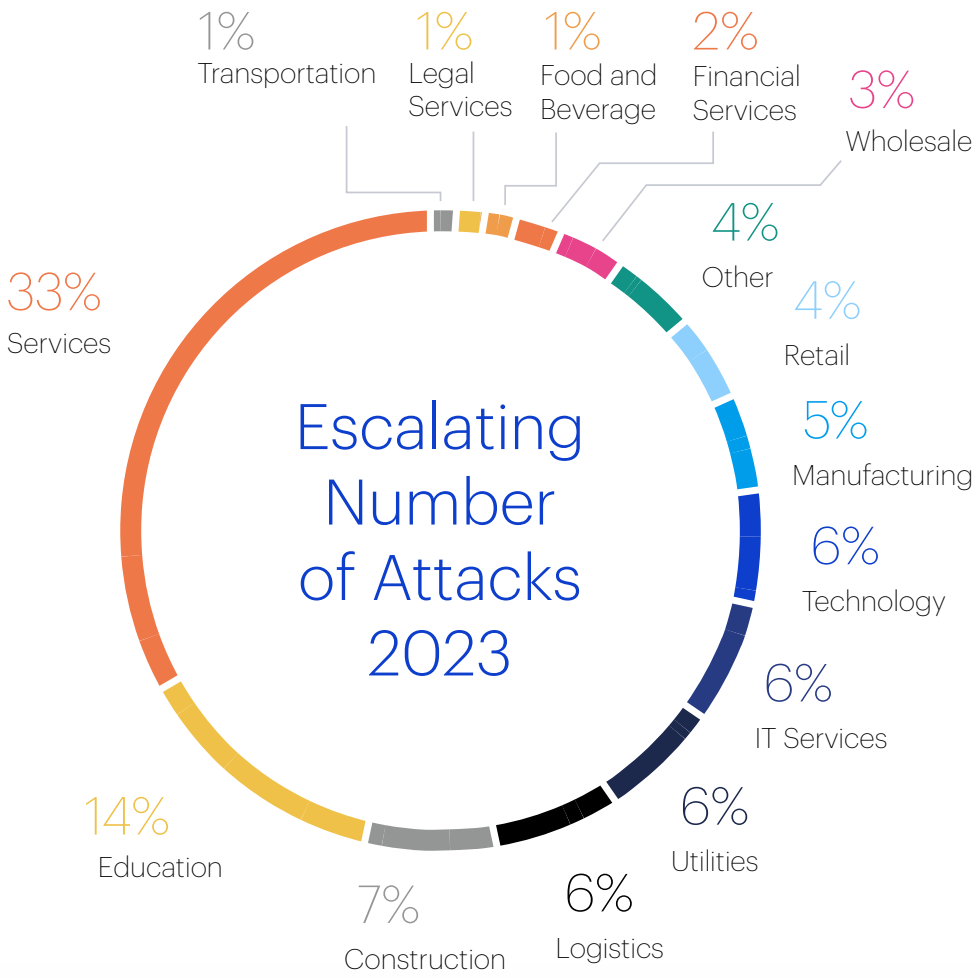


Although part of the increase can be attributed to new tactics and an increase in the number of gangs operating inside the UK, the primary cause seems to be an increase in activity by groups that are already active.

This can be seen clearly by examining how many groups carry out more than one known attack per month. The number has climbed steadily for a year, from just one in July 2022 to eight June 2023.

EDUCATION UNDER SIEGE

Over the last 12 months, education was the second most attacked sector in the UK behind services, suffering 14 percent known attacks—a far higher proportion than in other countries, including the US.



We first reported on this alarming trend in April, when we revealed that most of the trouble in UK education can be attributed to a single group, Vice Society, which was single-handedly responsible for 64 percent of all attacks on the sector.

Since April, the picture has changed, with some good news, and some bad. The good news is that Vice Society has only reported one attack on the UK education sector in the past three months.

The bad news is that the UK education sector remains a significant target for ransomware gangs, and the number of gangs recording attacks on UK education has increased from three in the six months from July to December 2022, to six between January and June 2023.

Over the last 12 months, education was

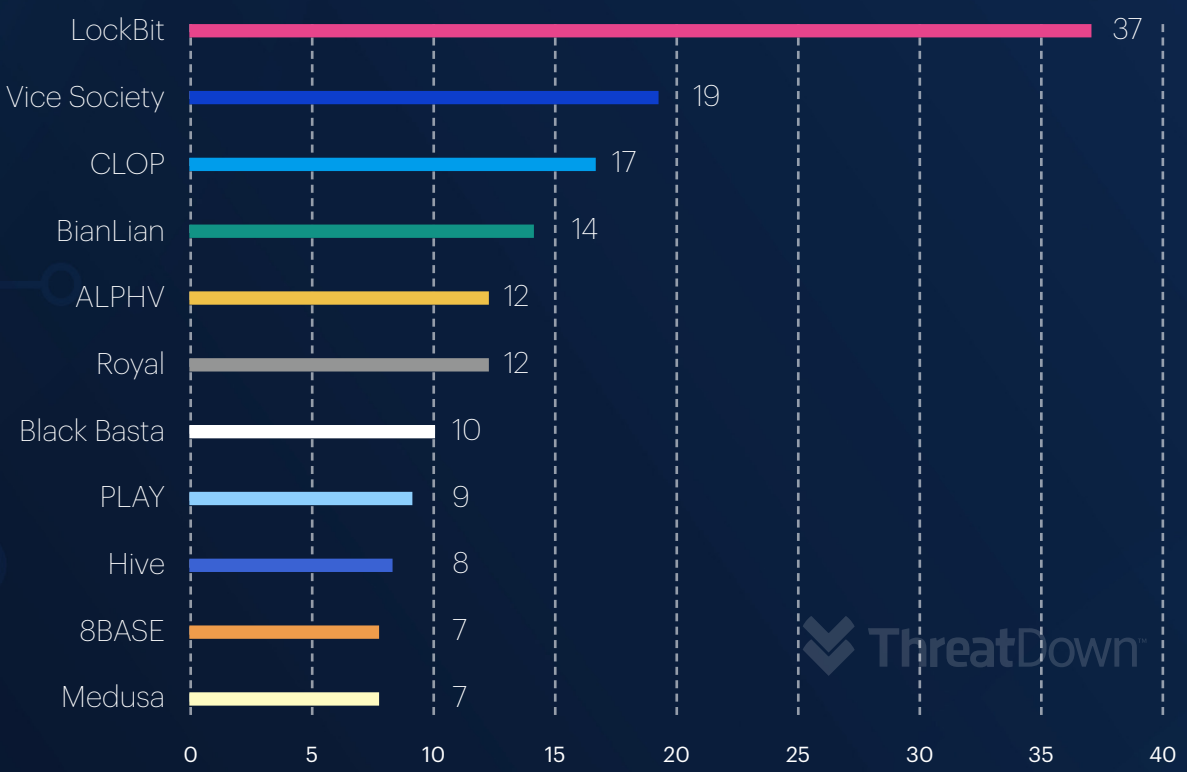
the second most attacked sector

in the UK ...

GANGS

In the last 12 months, Malwarebytes tracked 32 separate ransomware groups operating inside the UK, seven of which recorded 10 or more known attacks, including the group known as CLOP.

Attacks in the UK by the 10 most active ransomware groups
July 2022 - June 2023



The most active group in the UK for the past 12 months was LockBit, which is in line with its status as the global leader in ransomware.

The second and third most active groups have more of a story to tell. Vice Society ranks tenth globally over the last year, but it was the second most active gang in the UK during that time—largely because of its targeting of UK education.

The presence of CLOP in third position is remarkable and may foreshadow a change in ransomware tactics, and a potential escalation of the ransomware problem.

All but one of CLOP's known attacks occurred in March and June 2023, and yet it was so busy in those months it surpassed groups that were active for all 12 of months of the last year. The reason is that CLOP has been operating in a different way to the others.

For several years, criminals have relied on a Ransomware-as-a-Service (RaaS) model to scale their operations. Individual attacks require a significant investment of time and people, so ransomware groups sell their RaaS to gangs called "affiliates," which carry out the attacks.

> ... in the two months where CLOP was active, it far surpased LockBit's work rate.

For a year and a half, LockBit, which claims to have 100 affiliates, has been the most dominant form of RaaS both globally and in the UK, but in the two months where CLOP was active, it far surpassed LockBit's work rate.

It did this by scaling in a different way: Through the use of zero-day vulnerabilities.

In March, CLOP used a zero-day in the GoAnywhere MFT secure file transfer tool to break into victims' networks, and then in late May, after two quiet months, it returned to abuse a zero-day in Progress Software's file transfer tool MOVEit Transfer.

It's a feature of the ransomware ecosystem that when one group discovers a new and successful tactic, other groups are quick to follow. The last great change occurred in 2019 when the Maze ransomware group triggered a wholesale shift to so-called "double extortion"—using both encryption and the threat of data leaks to coerce victims.

CLOP's use of zero-days has the potential to create a similar shift. Whether it does or not will come down to a cold assessment of return on investment.

Malwarebytes' Threat Intelligence Analyst and ransomware specialist, Marcelo Rivero, regards CLOP's most recent campaign as only a partial success for the group, saying "From CLOP's perspective the campaign has achieved mixed success.

... CLOP's campaigns in 2023 have shown that ransomware gangs can now handle the cost and complexity of using zero-days.

While it exploited a previously unknown vulnerability, the generally low quality of the data stolen may have compromised its objectives."

What CLOP's campaigns in 2023 have shown is that ransomware gangs can now handle the cost and complexity of using zero-days. And when they do, the volume of attacks can scale far beyond what's possible with other approaches.

It is hard to escape the idea that we are watching the group trying to solve ransomware's scalability problem in real time.

Protecting your business from ransomware attacks

Attack Flow

Protection

ACCESS

RDP Brute Force

Vulnerability

Phishing

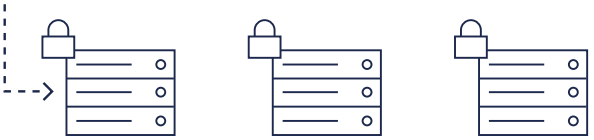
Brute Force Protection, **Patch Management**, and **Malicious Website Protection** target different forms of access.

INFILTRATION

Attackers escalate privileges and move throughout the network, targeting backups and security software.

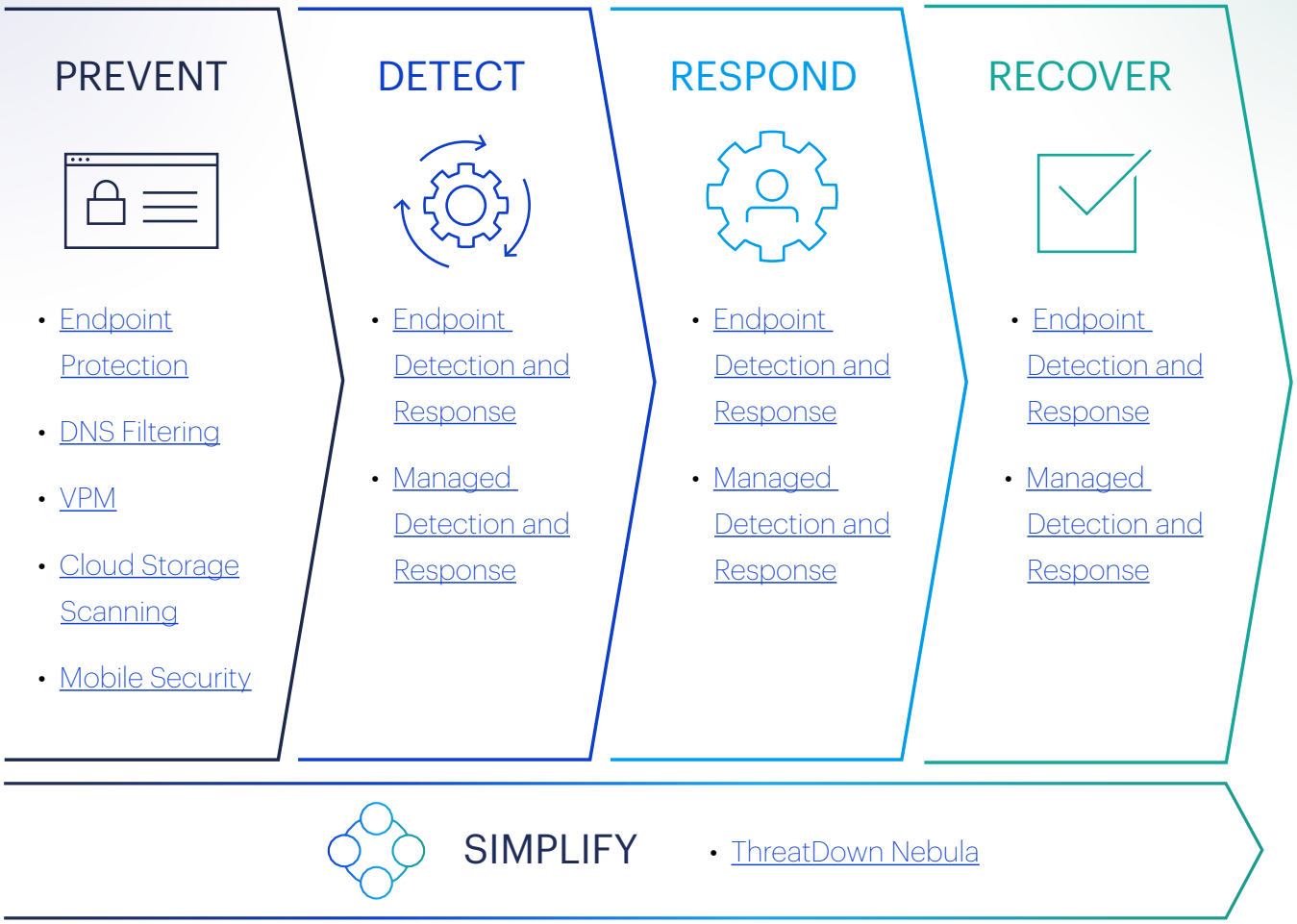
MDR can identify attackers as they operate inside your network, before they launch ransomware.

ENCRYPTION



EDR can detect ransomware, identify surreptitious encryption, and roll back affected files to an unencrypted state.

Solutions for every step in the threat lifecycle



EDR

Famous around the world for catching the threats that others miss, ThreatDown Endpoint Detection and Response (EDR) provides advanced protection with precise threat detection, proactive threat blocking, and thorough remediation, for both Windows and Mac, that earned the #1 ranking for Endpoint Protection by G2.

MDR

Small and medium-sized businesses, without dedicated around-the-clock threat experts, experienced in combating the cybercriminals responsible for ransomware and other advanced attacks, can now add Malwarebytes' own experts to their staff with ThreatDown Managed Detection and Response (MDR). Our MDR service provides powerful and affordable threat detection and remediation services with 24x7 monitoring and investigation that's purpose-built for resource constrained IT teams.

ThreatDown™
Powered by Malwarebytes

We're here to help

Learn more about today's most serious malware trends and threats—and how ThreatDown can help keep your organisation safe.

Learn more