2023 STATE OF RANSOMWARE

BETWEEN JULY 2022 AND JUNE 2023

→ The US was the most attacked country in the world, by far

→ It bore the brunt of a change in ransomware tactics based on zero-days

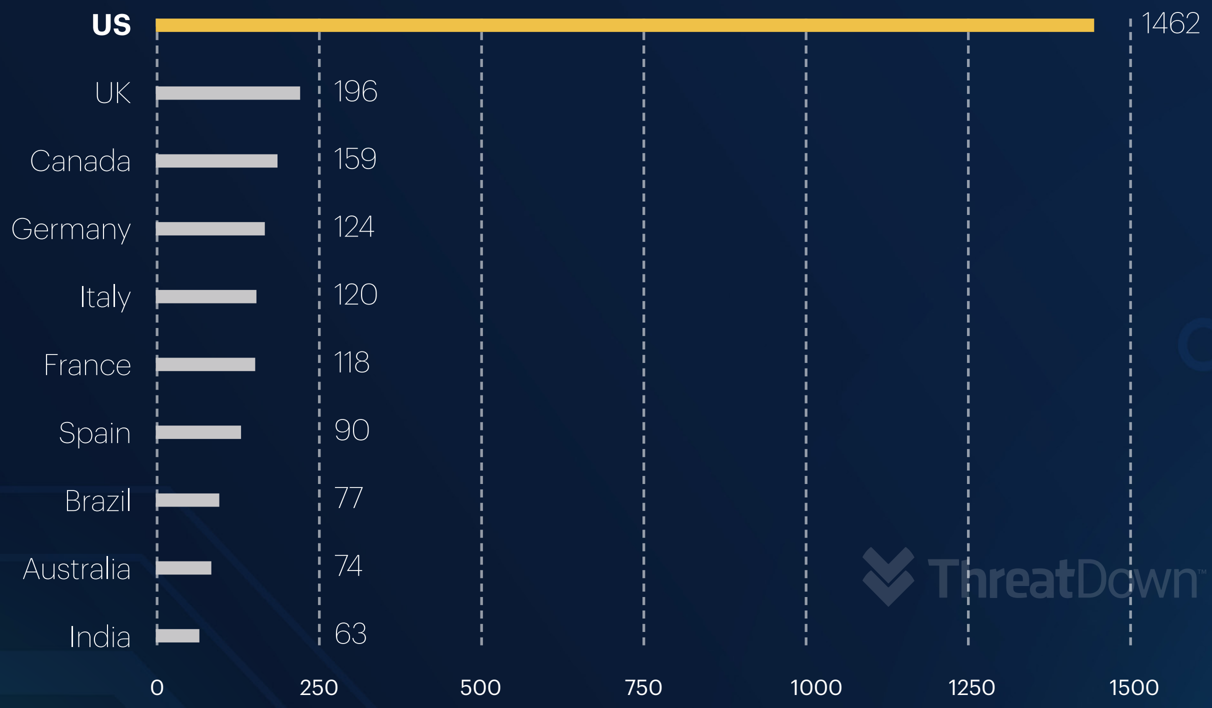
→ Its education and health sectors suffered more attacks than most countries

THE MOST ATTACKED COUNTRY IN THE WORLD

In the 12 months from July 2022 to June 2023, the US suffered 1,462 known ransomware attacks (and many more unreported ones), making it by far the biggest target for ransomware in the world.

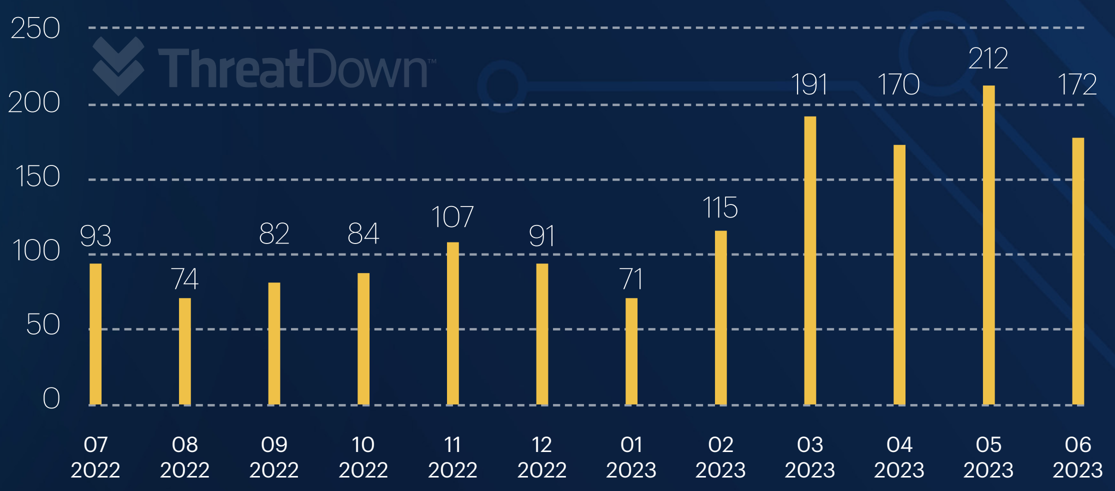
On its own, the US soaked up 43 percent of all known ransomware attacks—as many as the 22 next most affected countries combined, and 7.5 times more attacks than the second placed country, the UK.

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



Known attacks in the US per month

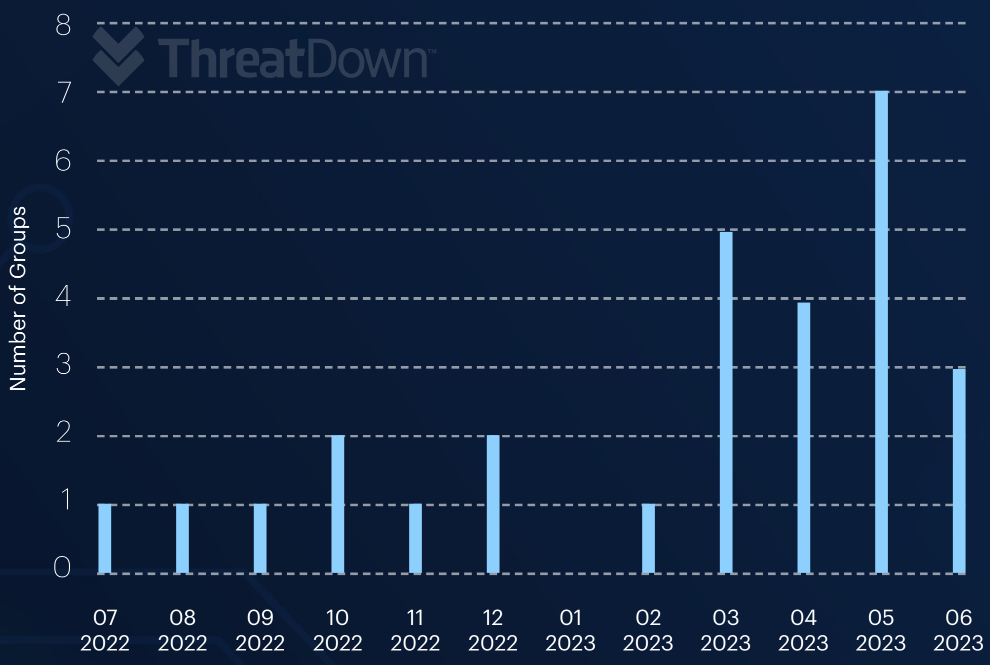
July 2022 - June 2023



The situation appears to be deteriorating, with the average number of monthly attacks climbing 75 percent between the first and second halves of the last 12 months.

Number of gangs reporting 15 or more known attacks per month in the US

July 2022 - June 2023

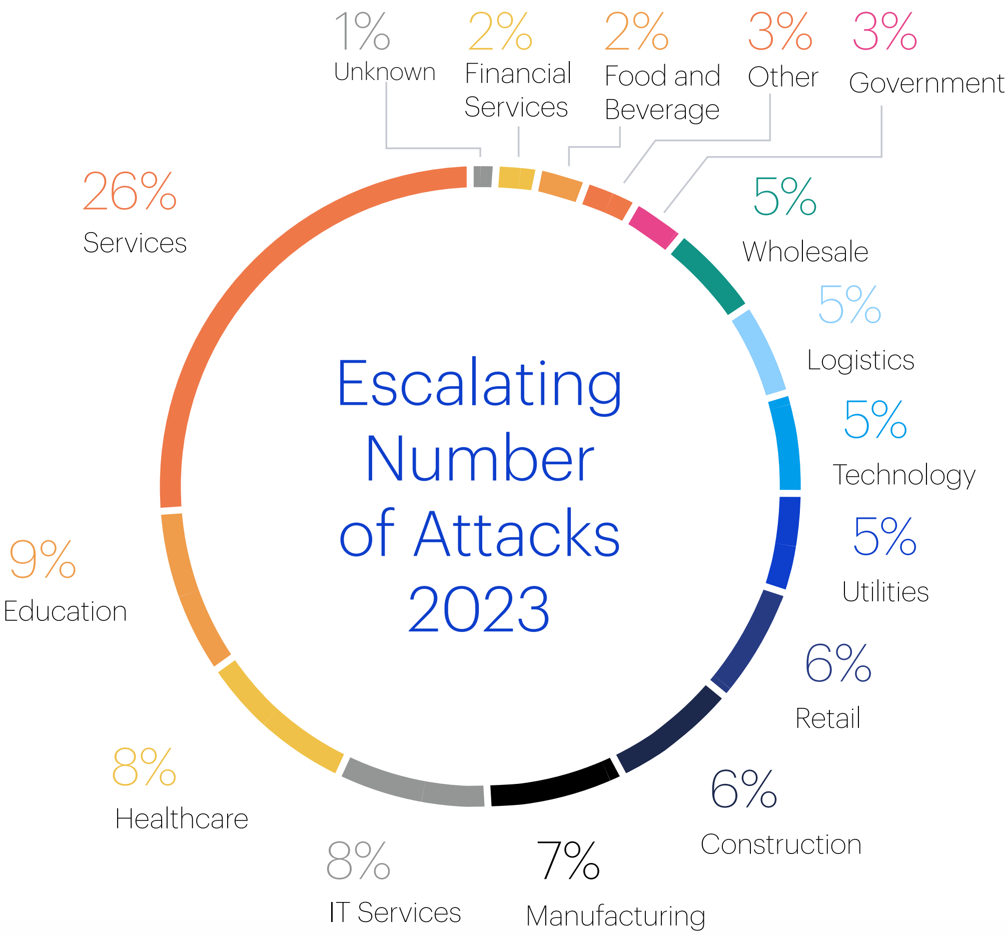


While the number of active groups in the US has increased over the last year, the escalation in the number of monthly attacks appears to be the result of existing ransomware groups being more active.

This can be seen by comparing the number of groups that carried out 15 or more attacks in a month during the last year. Between July and December 2022, only two groups ever managed it. Between January and June 2023 the maximum was seven.

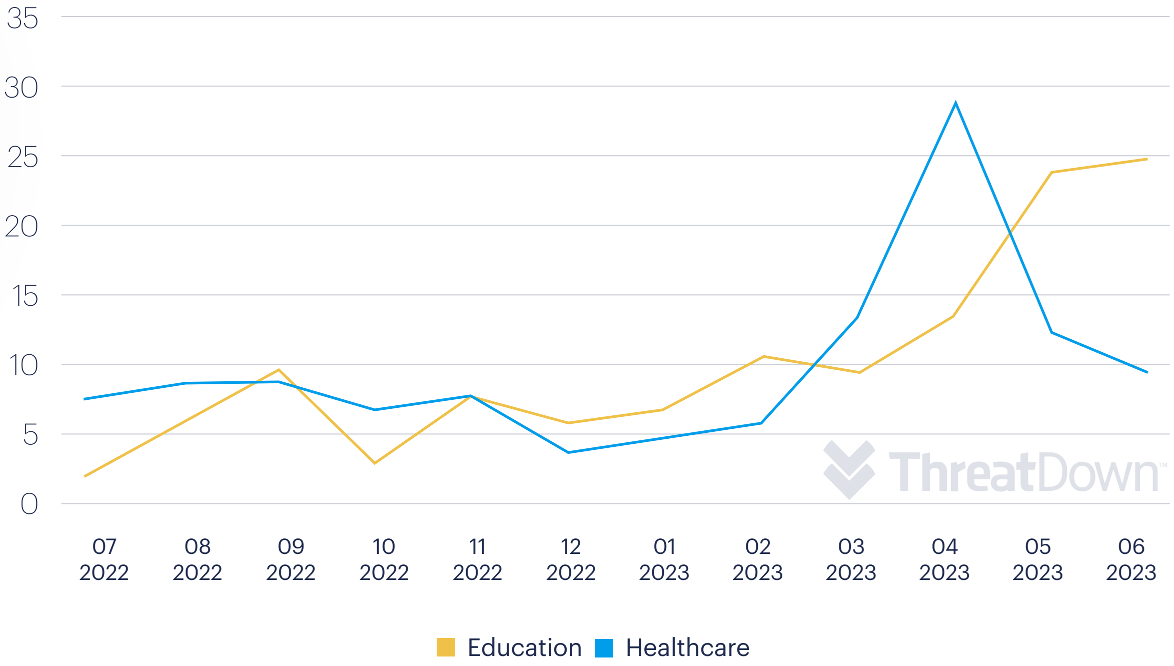
HEALTHCARE AND EDUCATION IN THE CROSSHAIRS

Over the last 12 months, education and healthcare were the most beleaguered sectors in the US outside of services. They received so many attacks that if they were countries, they would be the fourth and sixth most attacked in the world, on either side of Germany.



Both also appear to be facing an escalating number of attacks, with sharp rises in 2023.

Known ransomware attacks on education and healthcare in the US
July 2022 - June 2023



The presence of both sectors, so high in the rankings, is unusual and a cause for concern.

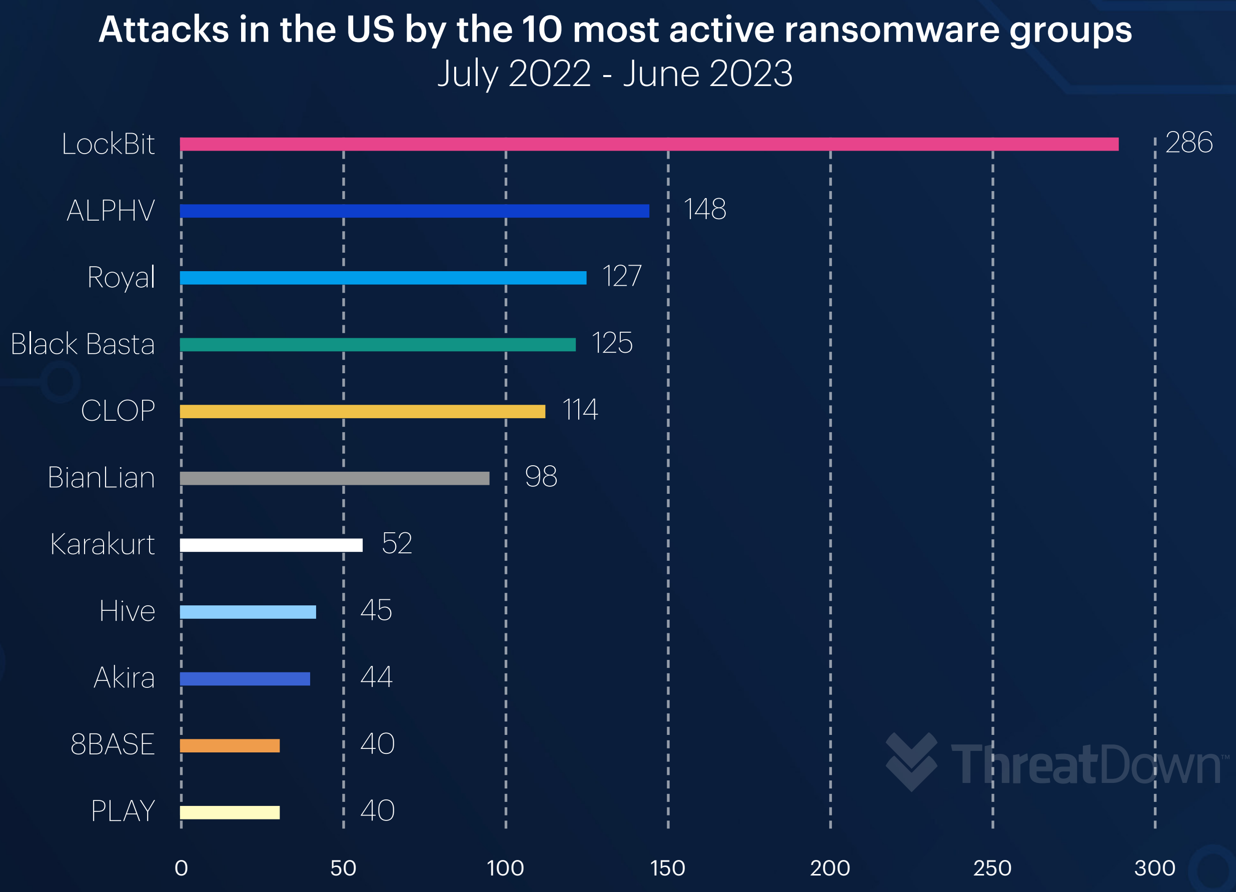
It's well established that the effects of ransomware attacks reach far beyond the organizations they target. In the case of education and healthcare, the effects are especially pernicious because they can impact the education of young people and the medical treatment of hospital patients.

For example, in October 2022, CommonSpirit Health, a Chicago-based non-profit hospital chain, had to shut down its systems after a severe ransomware attack that disturbed key hospital functions and affected 140 hospitals and more than 1,000 care sites in 21 states.

The attack occurred a month after the Los Angeles Unified School District (LAUSD), which serves over 640,000 students, was hit by ransomware.

RISE OF THE ZERO-DAY

In the last 12 months, Malwarebytes tracked 48 separate ransomware groups operating inside the US, five of which recorded more than one hundred attacks, including the group known as CLOP.



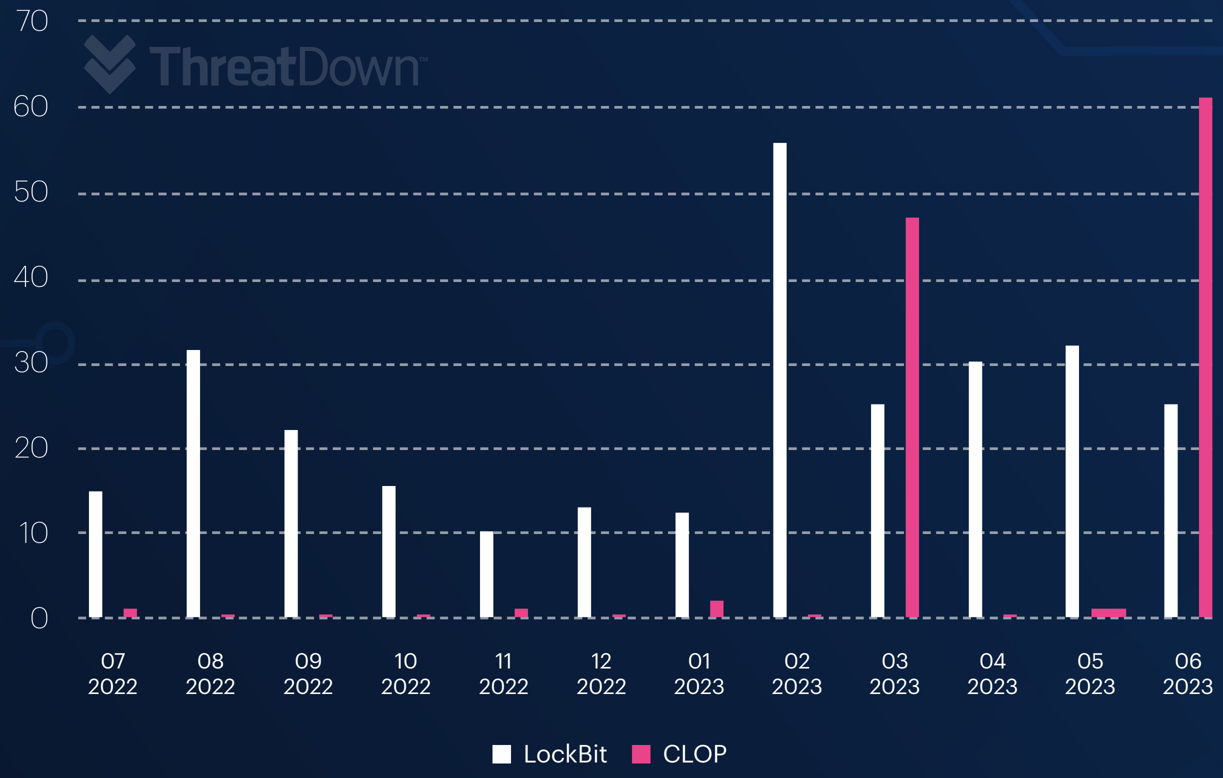
The presence of CLOP in fifth position in our top 10 ransomware may indicate a change in tactics and an escalation of the ransomware problem.

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.

For a year and a half, LockBit, which claims to have 100 affiliates, has been the most dominant form of RaaS in the US, averaging about 24 attacks per month.

However, twice this year, in March and June, LockBit's considerable rate of attacks was vastly exceeded by CLOP, which was otherwise dormant.

Comparison of monthly attacks by LockBit and CLOP
July 2022 - June 2023



In March, CLOP used a zero-day vulnerability in the GoAnywhere MFT secure file transfer tool to break into numerous victims' networks, chalking up 48 known attacks—almost double LockBit's total.

In late May, after two quiet months, CLOP returned, abusing a zero-day in Progress Software's file transfer tool MOVEit Transfer to compromise an even larger number of victims, again vastly exceeding LockBit's output that month.

It's a feature of the ransomware ecosystem that when one group discovers a new and successful tactic, others 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.

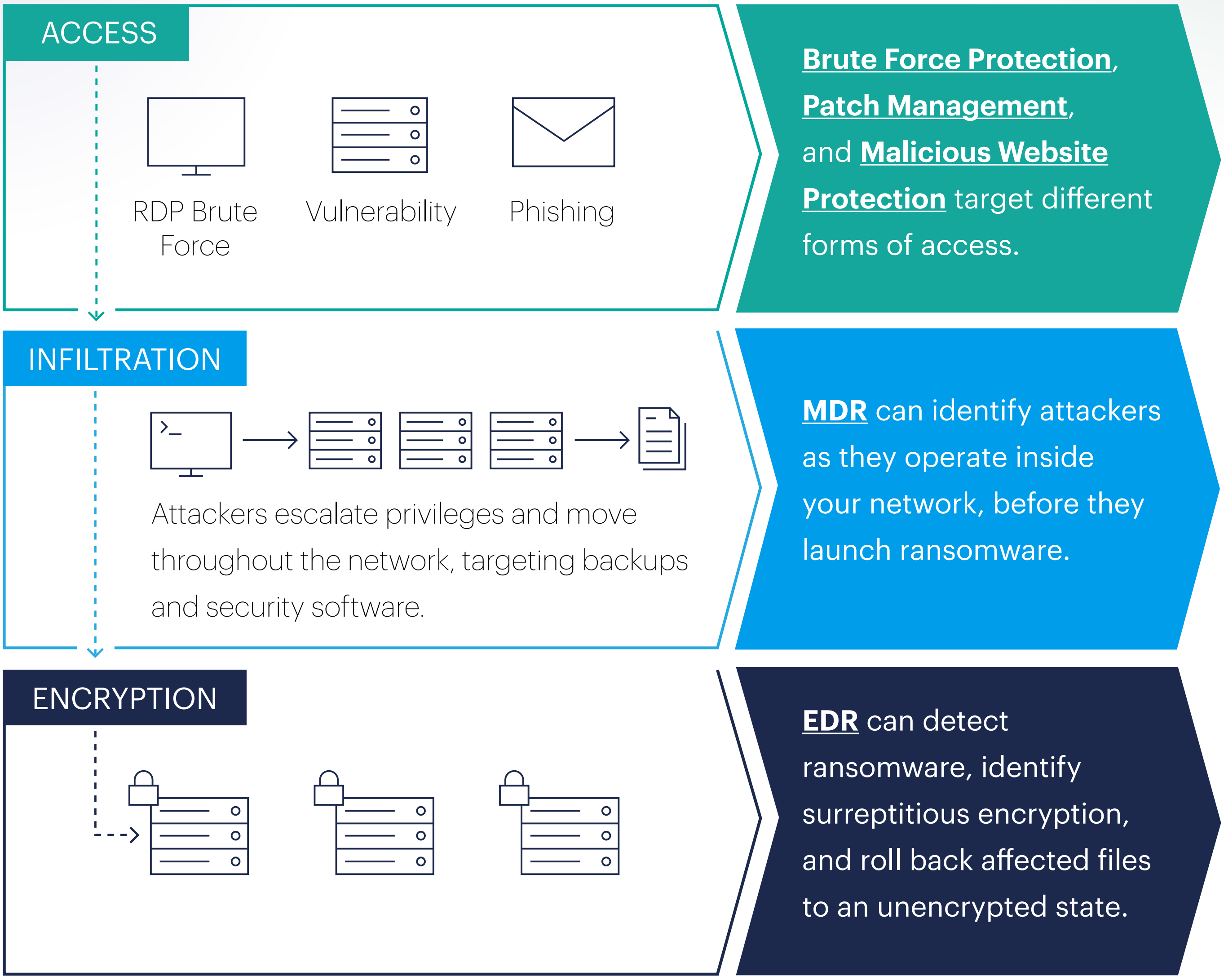
> ... CLOP used a zero-day vulnerability ... to break into numerous victims' networks, chalking up 48 known attacks ...

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. 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

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

INFILTRATION

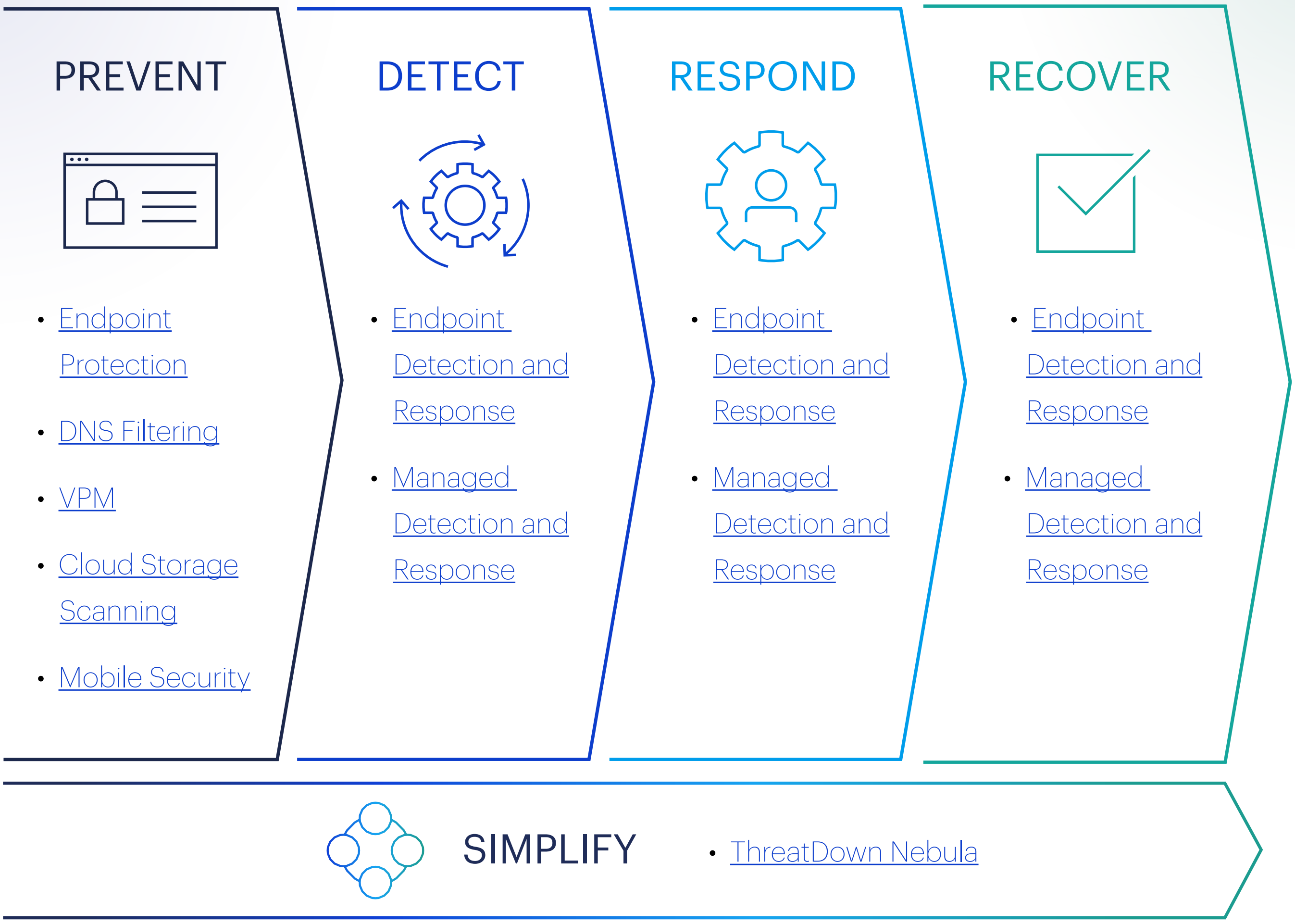
Attackers escalate privileges and move throughout the network, targeting backups and security software.

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



PREVENT

- Endpoint Protection
- DNS Filtering
- VPM
- Cloud Storage Scanning
- Mobile Security

DETECT

- Endpoint Detection and Response
- Managed Detection and Response

RESPOND

- Endpoint Detection and Response
- Managed Detection and Response

RECOVER

- Endpoint Detection and Response
- Managed Detection and Response

SIMPLIFY

- ThreatDown Nebula

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.

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 organization safe.

Learn more