ThreatDown
Powered by Malwarebytes

2024 ThreatDown State of Ransomware

A playbook to counter the latest ransomware gangs and attacks

Contents

Introduction

IT and security teams need to be smart with how they allocate their limited time and resources, and must be vigilant to changes in the threat landscape. In this report we explain how the broader ransomware ecosystem has changed in the last 12 months, how the tactics used by ransomware gangs have evolved, and how protection needs to adapt to keep pace.

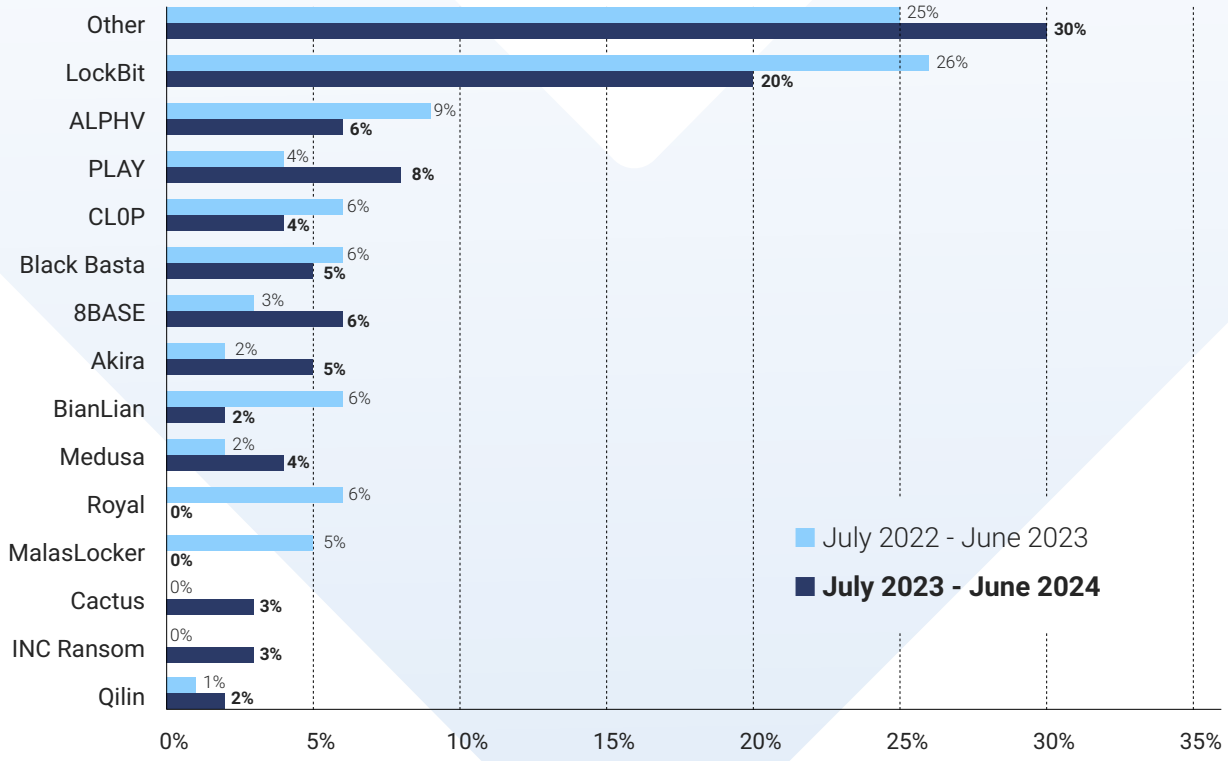
For several years, the number of known ransomware attacks has increased relentlessly, and the last twelve months were no different. Between July 2023 and June 2024, known ransomware attacks increased 33% year-on-year.

The growth in attacks was accompanied by a shift away from a small number of big gangs to a larger number of smaller gangs, suggesting that ransomware attacks are becoming easier and the barrier to entry for criminals has been lowered.

The share of ransomware attacks carried out by gangs outside the top 15 grew from 25% to 31%, while the dominant RaaS group, LockBit, saw its share of the pie shrink, even as it recorded an increase in attacks.

Pretenders to the number one position like PLAY, 8Base, and Akira all increased their activity significantly without ever coming close to matching LockBit's impact.

Known ransomware attacks by group
(July 2022 – June 2024)



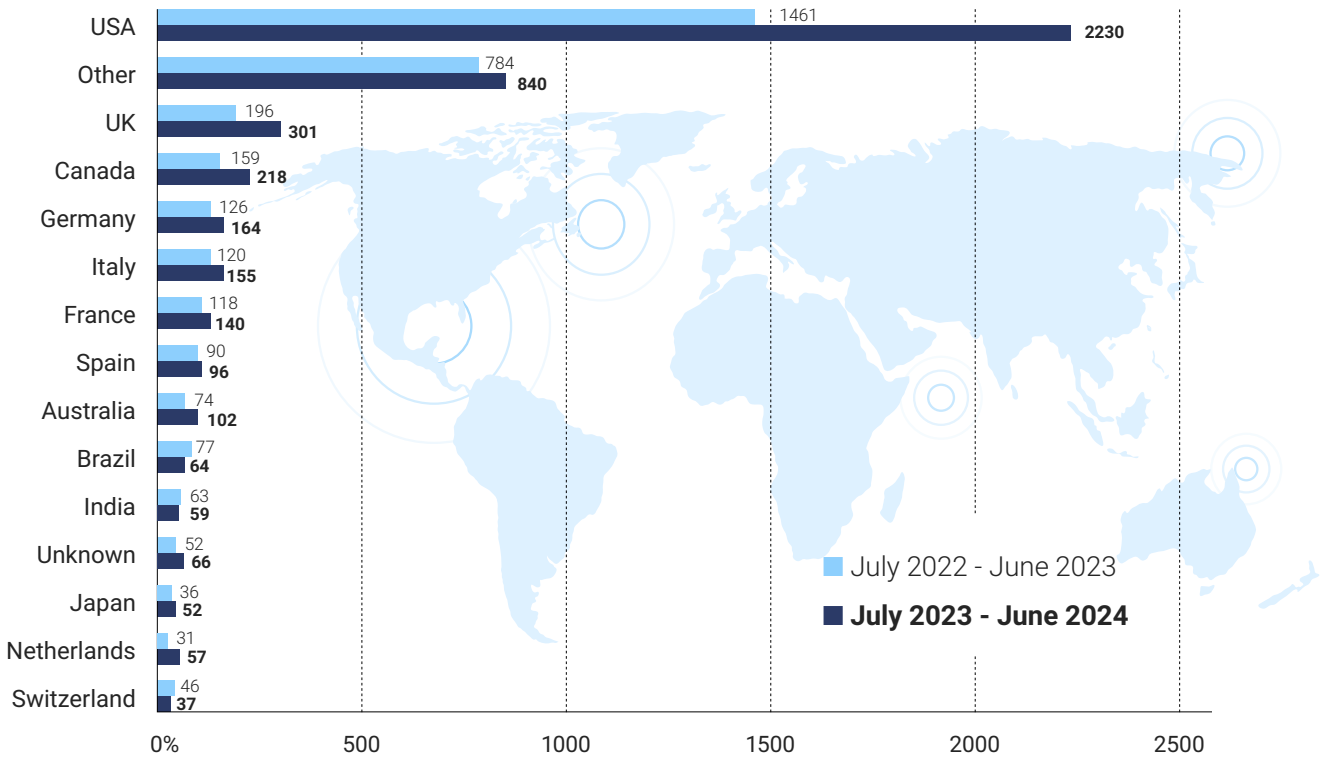
Attacks by country and industry

Ransomware activity increased in all the most targeted countries, with the USA seeing an enormous 63% hike in known attacks, and the UK an even larger 67% increase.

As attacks increased, ransomware payments passed $1 billion a year for the first time in 2023, while the average ransom payment climbed to $620,000, and the average cost of recovering from a ransomware attack hit $4.7 million.

The USA remains the epicenter of ransomware and now accounts for about half of all known attacks, while services remained the industry sector that suffers the most attacks, accounting for almost a quarter.

Known ransomware attacks by country
(July 2022 – June 2024)



Attacks by country and industry

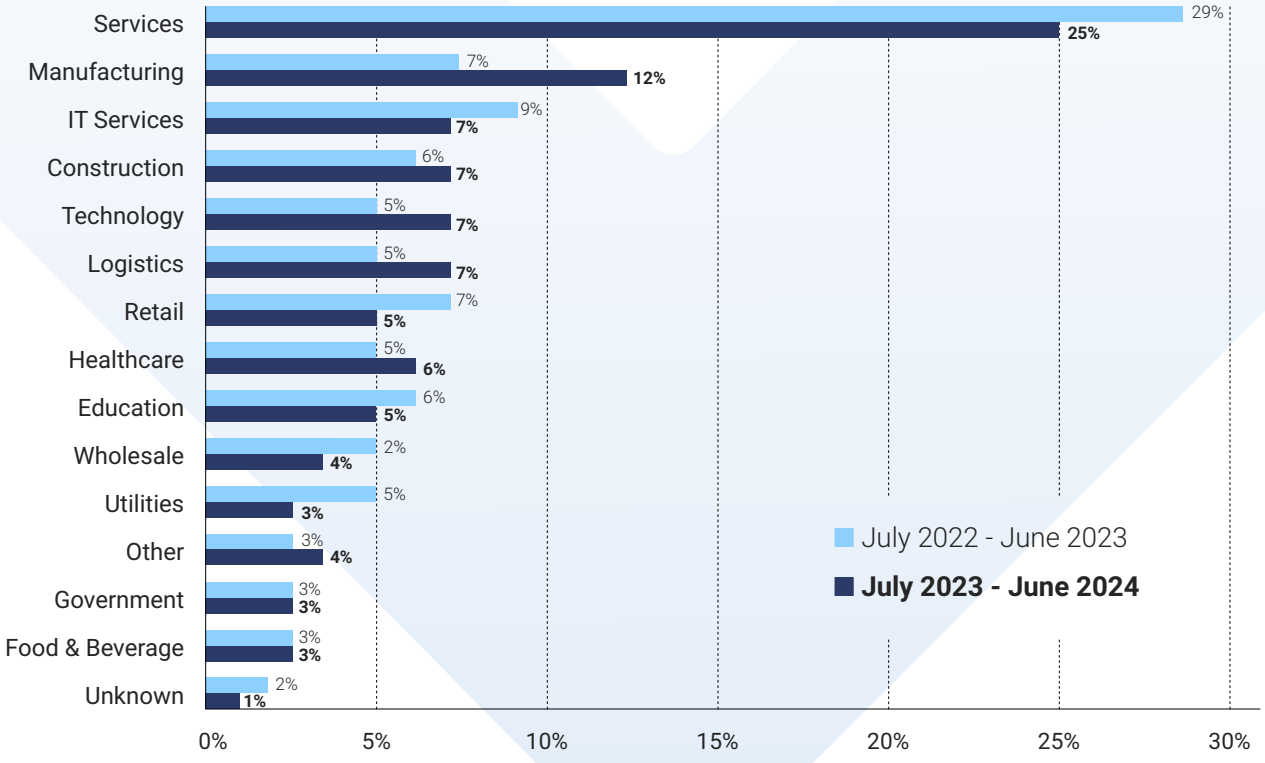
The extent to which different industry sectors are affected by ransomware has remained largely static over the last two years. Although, the relatively small year-on-year differences in attacks on healthcare and education hide significant peaks and troughs, and wide differences between countries.

Outside the USA, healthcare and education do not appear to be high priority targets for ransomware gangs, while inside the USA both receive special attention. The country accounts for 48% of all ransomware attacks worldwide but suffers 60% of the world's attacks on education and 71% of attacks on healthcare.

The one global exception to the otherwise stable picture of attacks in industry sectors over the last two years is manufacturing, which has seen a 71% year-on-year increase in attacks, with no obvious root cause.

The increase in manufacturing attacks has occurred gradually over time, in most countries, and is spread across multiple ransomware groups. Unlike attacks on education and healthcare in the USA, it's possible that the increase in global attacks against manufacturing is not the result of deliberate targeting.

Known ransomware attacks by industry sector
(July 2022 – June 2024)



Attacks by country and industry

The most likely explanation therefore is that the number of available targets in the manufacturing sector has increased over the last two years, perhaps because of increasing digitization within the sector.

If that is the reason, then the increase is a cautionary tale to any organization or industry sector that successful digital transformation should have cybersecurity embedded from the start. Ransomware gangs are experienced, global actors, and organizations of all kinds, no matter how recently they have digitized, need to be able to fight fire with fire by deploying similarly experienced defenders to watch their networks around-the-clock.

Known ransomware attacks on the manufacturing sector
(July 2022 – June 2024)

Changes at the top in the ransomware ecosystem

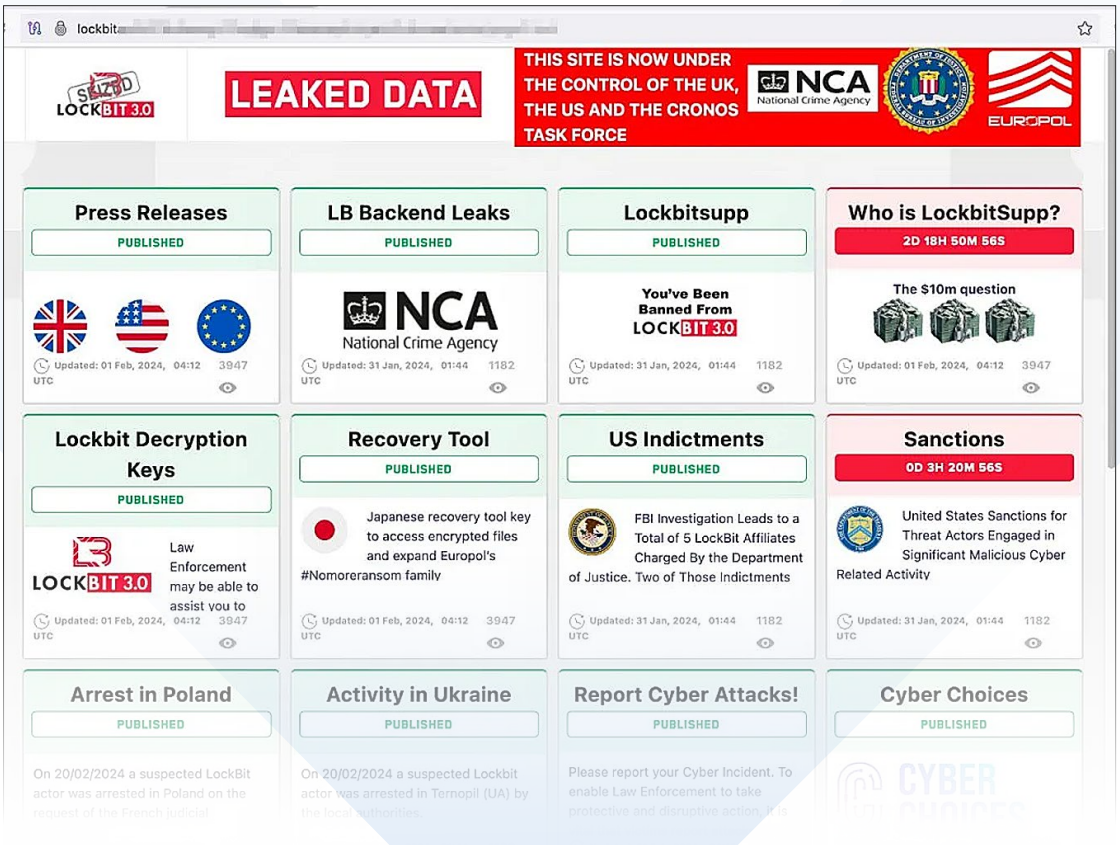
February 2024 is likely to be remembered for years as the month when the status of two of the most dangerous ransomware gangs in the world changed significantly.

LockBit has been the preeminent ransomware menace since the demise of Conti in spring 2022, but for the first time there are now reasons to doubt its longevity. On February 19, the ransomware gang's dark web site announced that it was under the control of an international law enforcement task force.

What followed was something quite unique in the annals of ransomware takedowns. Alongside the usual dry press releases, the law enforcement agencies responsible used the confiscated LockBit site to showcase the information they had acquired about the gang.

The "trolling" by law enforcement mimicked the way that ransomware gangs denigrate each other and looked designed to damage the LockBit brand by humiliating it in the eyes of its peers and affiliates.

Law enforcement used the compromised LockBit leak site to "troll" the gang



Changes at the top in the ransomware ecosystem

As well as taking over the leak site, law enforcement agencies took over LockBit's administration environment, recovering "a vast amount of intelligence", captured its source code, seized its data exfiltration tool, Stealbit, captured over 1,000 decryption keys, and froze 200 cryptocurrency accounts. 28 servers belonging to LockBit affiliates were taken down, and two "LockBit actors" were arrested in Poland and Ukraine, and two more users of LockBit were charged in the USA.

Three months later, in May 2024, law enforcement unmasked, indicted and sanctioned Dmitry Khoroshev, AKA LockBitSupp, the gang's leader.

Despite the disruption, LockBit remains active, although it appears to be diminished.

LockBit's main rival and perennial number two, ALPHV, created a vacancy at top of the ransomware heap in February 2024 after it ceased operations with a sloppily executed exit scam.

The gang stole the $22 million ransom payment paid by Change Healthcare to one of its affiliates and then attempted to cover its tracks by replacing its website with an FBI takedown notice (recycled from a real FBI action against the ALPHV gang in December 2023).

With ALPHV gone and LockBit's future uncertain, other gangs are certain to be trying to attract their affiliates and supplant them as the dominant forces in ransomware.

ALPHV recycled a genuine takedown notice to fake its own death in February

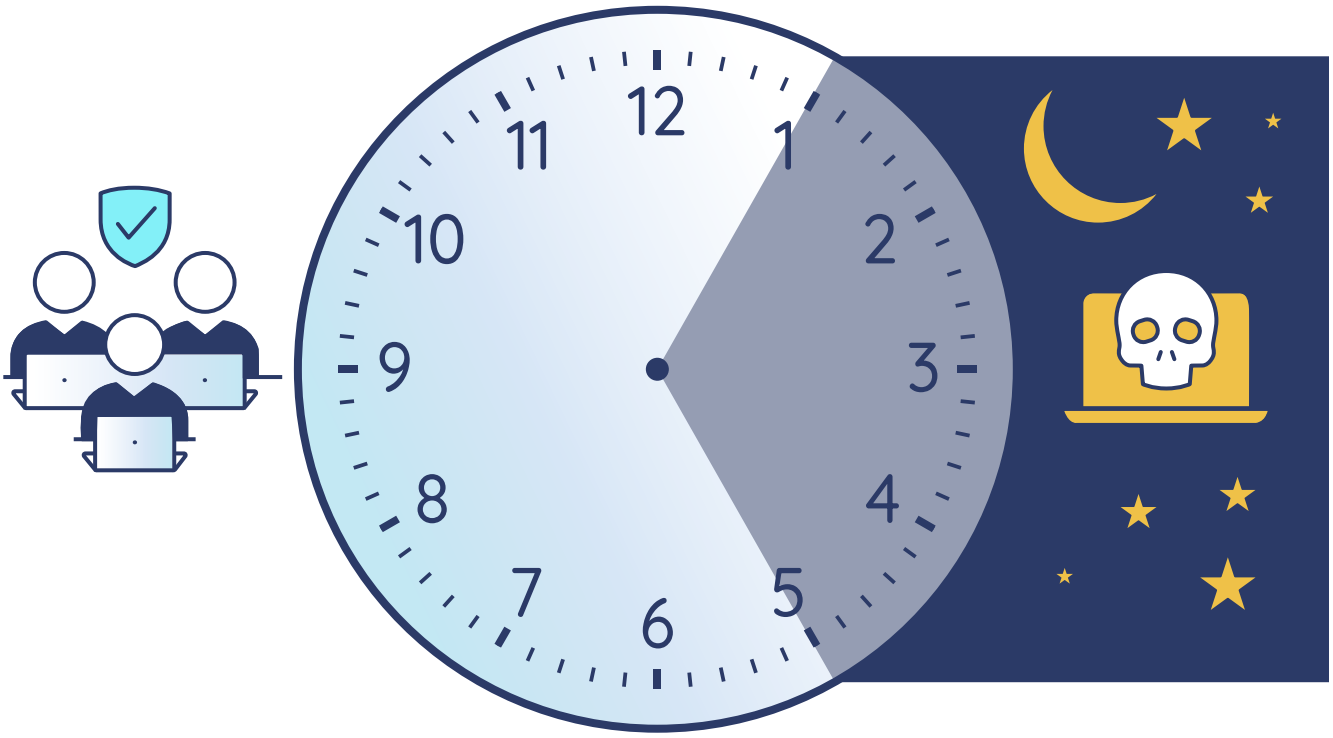
Top three ransomware trends

Changes in the ransomware ecosystem have been accompanied by changes in the tactics used by ransomware gangs. In what looks like a response to improving cybersecurity defenses and a decreasing willingness to pay ransoms, attackers have improved the speed and stealthiness of their attacks with three tactics.

1. More nighttime attacks

In the past year, ThreatDown Malware Removal Specialists (MRS) have witnessed an increase in ransomware gangs attacking companies on weekends and early hours of the morning—when they know IT staff won't be around. A majority of ransomware attacks the MRS team has handled in the last 12 months have occurred between 1 am and 5 am.

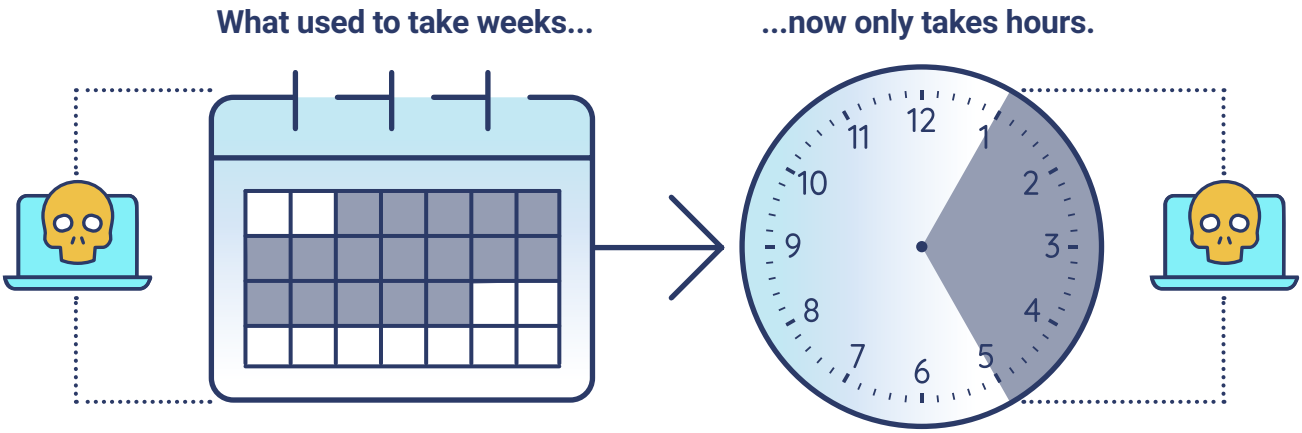
Most ransomware attacks happen at night, between the hours of 1 am and 5 am, while IT staff are asleep



Top three ransomware trends

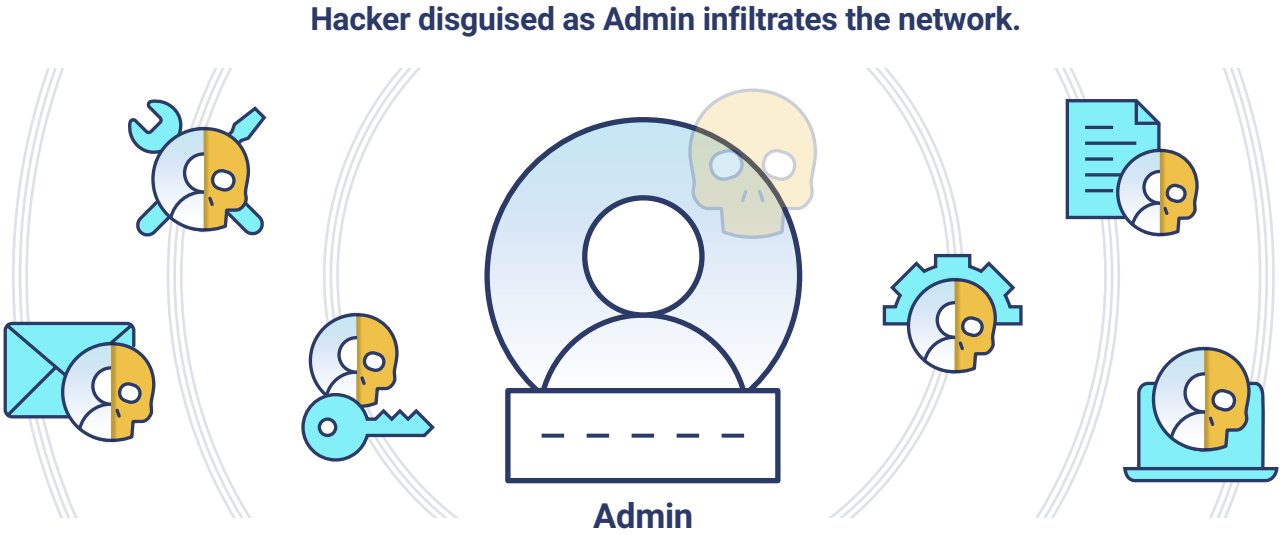
2. Attacks Are Getting Faster

Ransomware gangs are taking less and less time to encrypt and steal data than ever before. The entire ransomware attack chain—from initial access, to lateral movement, to data exfiltration and then encryption—has decreased from weeks to hours, according to ThreatDown Incident Response (IR) data.



3. Increase In Living Off the Land (LOTL) Techniques

Data from the ThreatDown Managed Detection & Response (MDR) team show more and more ransomware gangs using Living Off the Land techniques in their attacks, leveraging in-built system administration tools for malicious purposes. Recent customer incidents from top gangs such as LockBit, Akira, and Medusa reveal that most of the modern ransomware attack chain is now composed of LOTL techniques.



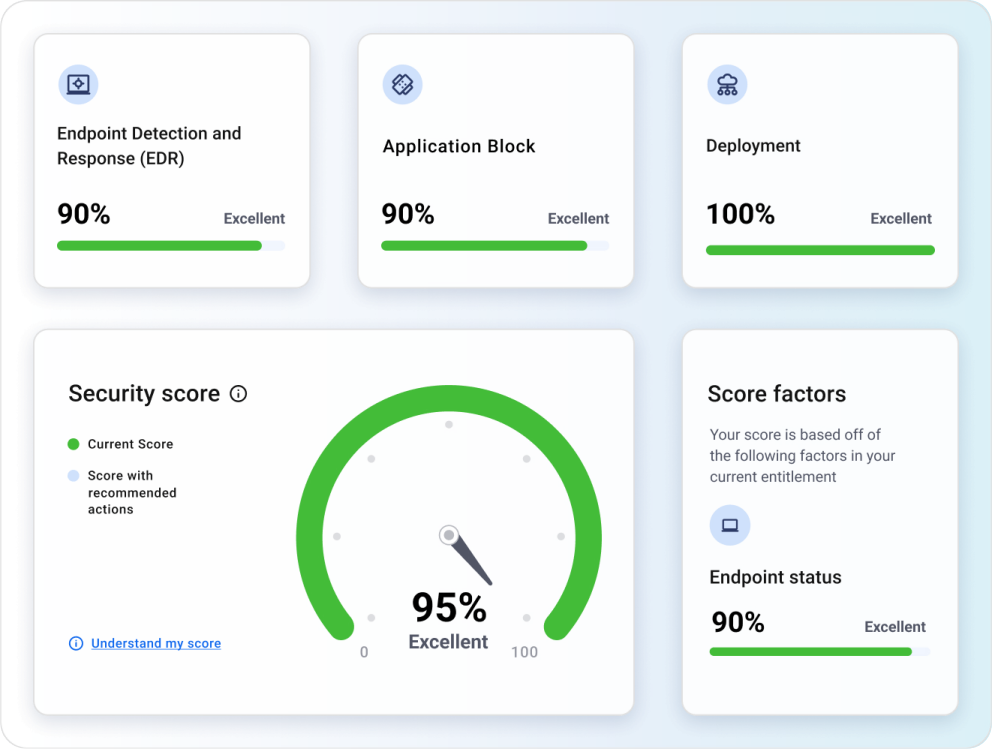
Conclusion

Superficially, the changes in ransomware over the last year leave little to be cheerful about: attacks are increasing, the barrier to entry for new cybercriminals appears to lowering, and attacks are getting faster and more stealthy.

The good news hidden within the bad is that recent changes in ransomware tactics are a response to organizations improving their defenses. Technologies, like endpoint detection and response (EDR), can identify attackers before they launch malware have pushed ransomware gangs to work more quickly and put more effort into hiding themselves.

The question that all organizations must now answer is who is going to watch their EDR and respond with urgency to alerts at night, over the weekend, or during holidays, when ransomware gangs are at work.

Increasingly, the answer for organizations is managed detection and response (MDR), a service that provides 24x7x365 threat monitoring, investigation, and remediation by expert security analysts without the need to recruit and maintain a security operations center.



Learn more about how ThreatDown MDR can help your business.

Talk to an expert

ThreatDown™
Powered by Malwarebytes

3979 Freedom Circle, 12th Floor
Santa Clara, CA 95054 USA
sales@threatdown.com