UNDER THE RADAR

Darren Williams *explains why the threat from the ransomware epidemic is five times greater than you realise*

Few criminal enterprises have reshaped the cyber landscape as profoundly and persistently as ransomware. Its impact has been so widespread that businesses and service providers across every major industry sector have suffered the reputational and financial fall out of a major attack; from retailers and manufacturers forced into costly and prolonged shutdowns, to hospitals scrambling to provide patient care. But the incidents constantly making the headlines represent only a small fraction of what is really happening.

In fact, BlackFog research has found that 86 percent of worldwide ransomware attacks in 2025 were never publicly disclosed. The incidents dominating the news cycle are the tip of the iceberg and, below the waterline, thousands more organisations are suffering the consequences of an attack. It's the hidden side of the threat landscape in which data is stolen and payments are made without a single mention in the press, regulatory notice or public acknowledgement.

This matters for everyone, from security teams and boards at individual enterprises to governments, law enforcement agencies and policy makers. We cannot make real headway against a fast-moving, well-resourced criminal ecosystem if we're only seeing a carefully filtered version of the evidence. Understanding the true scale of ransomware determines the defences we build, the regulations we write and the resources we commit. This means shining a light on the trends that go under the radar.

Ransomware has become a favoured weapon for state-backed threat actors seeking to disrupt opponents

A decade ago, ransomware was largely opportunistic – crude attacks on individual machines, demanding a few hundred pounds to unlock files. What we face now is something categorically different: a structured criminal industry with specialist groups, affiliate networks, tiered pricing and sophisticated business models. It has also become a favoured weapon for state-backed threat actors seeking to disrupt opponents without firing a shot.

The scale of growth reflects the interplay of these two forces. In 2025, BlackFog tracked 1,174 publicly disclosed incidents, which represents a remarkable 49 percent year-on-year growth. This is nearly a four-fold increase compared with the 2020 figures.

The number of attacks represents both more agile and organised groups that can strike quickly and easily, as well as the growing number of players in the field. There were 130 confirmed groups active in 2025, including 52 that emerged during the year. While top players like Qilin and Akira claimed the lion's share of incidents between them, newcomers such as Sinobi, Dire Wolf and World Leaks accounted for most of the attack volume between them.

Yet activity figures reveal only the visible layer of the problem. By examining evidence from ransomware leak sites, we have mapped the thousands of additional victims captured through official disclosures, which point to an ecosystem far larger than public statistics suggest.

ALL CHANGE

Numbers alone don't capture how fundamentally the nature of these attacks has changed. While ransomware attackers were once primarily focused on locking systems, scrambling files and demanding payment to restore access, that process is increasingly a sideshow.

Instead, the research shows that the vast majority (96 percent) of ransomware attacks now involve data exfiltration. Criminals aren't merely locking doors; they're first making off with the building's contents. The threat of data publication has now become their most potent weapon.

This shift fundamentally changes the economics of ransomware because, while encrypted systems can often be restored from backups, the theft of data poses a long-term risk that follows organisations well beyond the immediate crisis.

Stolen information immediately gives attackers a bargaining chip that they can hold indefinitely to trade, leak or weaponise in future attacks – regardless of whether the victim pays. Even if victims refuse to pay, the attackers still win.

While large-scale, disruptive encryption attacks remain a threat, organisations must be prepared for campaigns that focus on quiet, methodical extraction. Attackers prioritise stealth, speed, and data theft to claim their prize before victims can react.

Delving into ransomware leak sites, where criminal groups publish the names of victims whose data they claim to have stolen, reveals the true extent of the challenge. In 2025 alone, 7,079 organisations appeared on these leak sites, far exceeding the number of publicly disclosed incidents.

The shift toward data exfiltration is likely contributing to the number of attacks that go unreported. When criminals prioritise data theft rather than disabling systems, attacks can unfold with far less visible disruption, making them easier to conceal.

National and industry-specific regulatory frameworks stipulate an organisation's responsibilities when it comes to reporting cyber incidents that impact essential services and breaches that involve personal data. However, where incidents fall outside of the scope of these requirements, there is considerably less obligation – and often less incentive – to report attacks.

Reputational pressure plays a significant role in this decision. Public acknowledgement of a ransomware attack risks damaging customer trust and unsettling investors and, faced with these consequences, many organisations choose instead to resolve incidents quietly, whether through containment or direct negotiation with attackers.

86 PERCENT OF GLOBAL RANSOMWARE ATTACKS IN 2025 WERE NEVER PUBLICLY DISCLOSED

The disclosure issue also appears to be worsening with time and we noted that the number of unreported incidents increased by 37 percent in 2025 compared with the previous year. It's also notable that many of the largest ransomware players claim a large share of undisclosed attacks. The Qilin group, for example, was behind 99 officially reported attacks last year, but at least 1,016 more flew under the radar. This means the scale of unreported attacks may increase as threat groups grow in size and prominence.

The gap between disclosed and undisclosed ransomware attacks represents a serious challenge for governments, businesses and the wider security community, undermining evidence-based policymaking by masking the true scale and dynamics of the threat.

Policymakers rely heavily on reported incidents to shape national cyber strategies, allocate resources and design regulatory frameworks. Breach disclosures, law enforcement reports and threat intelligence all influence how risk is assessed. If these sources capture only a fraction of actual attacks, their perception of the threat landscape becomes distorted and decision-makers may underestimate both the scale and trajectory of the threat.

We could compare it with the early days of the COVID 19 pandemic, where a lack of case reporting made it difficult for health authorities to accurately gauge the spread and work to contain the virus. Just as a lack of data affected virus response plans, under reporting doesn't just hide a problem, it perpetuates it as the lack of visibility also hinders the work of security researchers and threat intelligence teams. Analysts depend on incident data to identify emerging attack techniques, track ransomware groups and understand which sectors are being targeted most aggressively, so undisclosed incidents mean valuable intelligence about attacker behaviour is lost.

The reporting gap can also affect how individual organisations perceive their risk. If ransomware incidents appear lower than they truly are, board members may underestimate the likelihood of an attack or underinvest in cyber defences.

Given its scale and reach, ransomware now firmly sits on the national security agenda. The threat is intensified by the fact that critical sectors are increasingly vulnerable, and attacks on Critical National Infrastructure (CNI) can have a significant impact on essential national services and the safety of citizens. BlackFog's research found that healthcare organisations and government bodies were two of the most targeted sectors in terms of publicly disclosed attacks last year.

AS MUCH AS 96 PERCENT OF RANSOMWARE ATTACKS INVOLVE DATA EXFILTRATION

There's a further economic impact, which can amount to millions in lost revenue, and which trickles down through the supply chain of companies brought to a standstill by a ransomware attack.

The aftermath of the attack on Jaguar Land Rover, the most costly cyberattack in the UK, is believed to have cost the UK economy a staggering £1.9-billion and affected over 5,000 companies in its extended supply chain.

Improving global reporting standards will take time, but organisations can take practical steps today to reduce their exposure to modern ransomware tactics. The most important shift is recognising that data theft, not encryption, is now the primary objective in most ransomware attacks. Encryption is often only a distracting smokescreen and security teams that focus their defences on keeping systems running may be fighting the wrong battle entirely.

As such, security teams must prioritise stopping sensitive data from leaving the network in the first place. This relies on the ability to accurately detect indicators, such as unusual outbound data transfers or spikes in network traffic. These are some of the clearest signs that attackers are attempting to extract valuable information before launching an extortion campaign.

Early-stage detection is equally critical here because many attacks begin with seemingly routine events, such as suspicious login attempts, repeated multi-factor authentication prompts, or unexpected data movement between systems. The earlier these signals are detected, the better the chance of identifying intrusions before attackers gain leverage. Deploying anti data exfiltration (ADX) technology will also make it much less likely that attackers can slip away with critical data.

Business and security leaders within organisations must take matters into their own hands to defend against ransomware and data exfiltration. But there is also much that can be done on a broader scale.

Greater collaboration between organisations, industry groups and government agencies can help close the intelligence gaps created by under reporting, allowing defenders to build a clearer picture of how ransomware groups operate. The more information is shared, the harder it is for threat actors to hide.

Each organisation that chooses not to report may be acting in their own interests to protect their reputation and avoid regulatory scrutiny, but the wider impact is a blind spot that benefits attackers far more than defenders.

Until we recognise the real extent of the problem, we risk fighting only the shadow of the ransomware threat rather than the reality of the threat itself. The attackers know exactly how much damage they can cause, and security decision makers must understand this too to have a chance at building the right defences ●

Darren Williams is Founder and CEO at BlackFog.

The most costly cyberattack in the UK – the attack on Jaguar Land Rover – cost the UK economy £1.9-billion

Picture credit: Land Rover/MENA