DragonForce Ransomware Explained: Origins, Cartel Model, Real Attacks and Defence

Imagine a franchise restaurant chain where the head office supplies the recipes, the kitchen equipment, and the customer-service desk, while local owners cook and serve under their own signboards. Replace the food with stolen data and locked computers, and you have a fair picture of how **dragonforce ransomware** operates in the criminal world. This guide walks you through its history, business model, notable attacks, technical behaviour, and practical defences, using simple examples and named sources so you can verify what you read. Whether you are a student, an IT administrator, or a business owner, you will finish with a clear understanding of the threat and the steps that reduce your risk.

What Is DragonForce? The Short Answer

DragonForce is a ransomware-as-a-service (RaaS) operation, which means its operators rent malicious software and support systems to affiliates who carry out the actual break-ins. It first appeared in late 2023 and later rebranded itself as a cartel to attract more partners and compete with larger extortion brands. Victims are pressured twice: their files are encrypted, and then their stolen data is threatened with public release on a dark web leak site. As of the end of

August 2026, the group's leak site had publicly claimed 645 victims across 65 countries, although such figures reflect criminal claims and not verified infections. Malware NewsDeXpose

Origins and Hacktivist Roots

Researchers describe the operation as beginning as a pro-Palestine hacktivist collective based in Malaysia before it pivoted toward profit-driven ransomware. Analysts who profile the **dragonforce ransomware group** often stress that this shift from ideology to income is a classic pattern, because activism gives way to commercial extortion once the profits become obvious. The group first gained visibility on underground forums such as BreachForums, RAMP, and Exploit before it built a formal affiliate programme. Malware NewsPrevent-ransomware

How the Cartel Business Model Works

In March 2025 the operators announced that they would run as a ransomware cartel rather than as a single closed gang. Under a **dragonforce ransomware cartel** structure, affiliates can deploy their own malware or brand while using the central infrastructure, including shared payloads, servers, and negotiation portals. Think of it as a shopping-mall landlord who provides the building, security, and payment counters while each shop keeps its own name and customers. This design lowers the technical barrier for newcomers and makes attribution harder, because one set of infrastructure can sit behind many different logos. Acronis

White-Label Branding and RansomBay

The white-label service, reported under the name RansomBay, lets partners generate customised payloads and tailor attacks to different environments. Acronis researchers linked variants such as Devman and Mamona to this affiliate-branding approach. As a result, defenders may see different ransom notes and leak sites even when the same underlying infrastructure sits behind the incidents. Prevent-ransomwareAcronis

Revenue Split and Data Analysis Service

Public threat profiles describe an 80/20 revenue split in favour of affiliates. A reported "Data Analysis Service" audits stolen files from large targets and drafts extortion call scripts and pseudo-legal threats to speed up payment. In simple terms, the criminals now offer consulting, which shows how professional this underground economy has become. HalcyonProven Data

The 2025 UK Retail Attacks: A Real-Life Example

The best-known case study is the wave of attacks on British retailers in spring 2025, which hit Marks and Spencer, Co-op, and Harrods within a matter of weeks. Researchers concluded that the intrusions showed tradecraft consistent with Scattered Spider, which gained access before the DragonForce payload finished the job. The episode shows how a **dragonforce ransomware cartel** partnership can combine one crew's skill at getting in with another crew's tools for locking systems. Shoppers saw empty shelves, paused online orders, and payment

problems, which turned an invisible cyber event into a very visible everyday disruption. DeXpose

Social Engineering as the Door Opener

Public reporting on the retail incidents pointed toward social engineering, such as convincing help-desk staff to reset credentials, rather than a rare software flaw. This matters because no firewall can stop a convincing phone call unless employees are trained to verify who is really calling. A simple lesson for any office is to require call-back checks, and to make multi-factor authentication resets depend on manager approval.

Business Impact and Lessons

Marks and Spencer later said the incident would cost it hundreds of millions of pounds in lost profit, and its online ordering was paused for weeks. Such figures explain why company boards now treat ransomware as a business continuity issue and not only as an IT problem. The practical lesson is that recovery planning, supplier communication, and manual fallback processes deserve the same attention as prevention.

Technical Profile: Payloads, Tactics, and Tools

Security analysts report that the payload is built primarily from leaked source code associated with LockBit 3.0 (Black) and Conti, which explains why its behaviour looks familiar to experienced incident responders. Because those builders leaked publicly, dragonforce ransomware does not need to invent new encryption from scratch and can focus its effort on access and extortion. Typical intrusions follow the double extortion pattern, where attackers exfiltrate sensitive files before encrypting servers, so victims face both downtime and a data-leak threat. Researchers have also observed a custom implant called Backdoor.Turn that abused Microsoft Teams infrastructure to hide its command-and-control traffic. Proven DataDeXpose

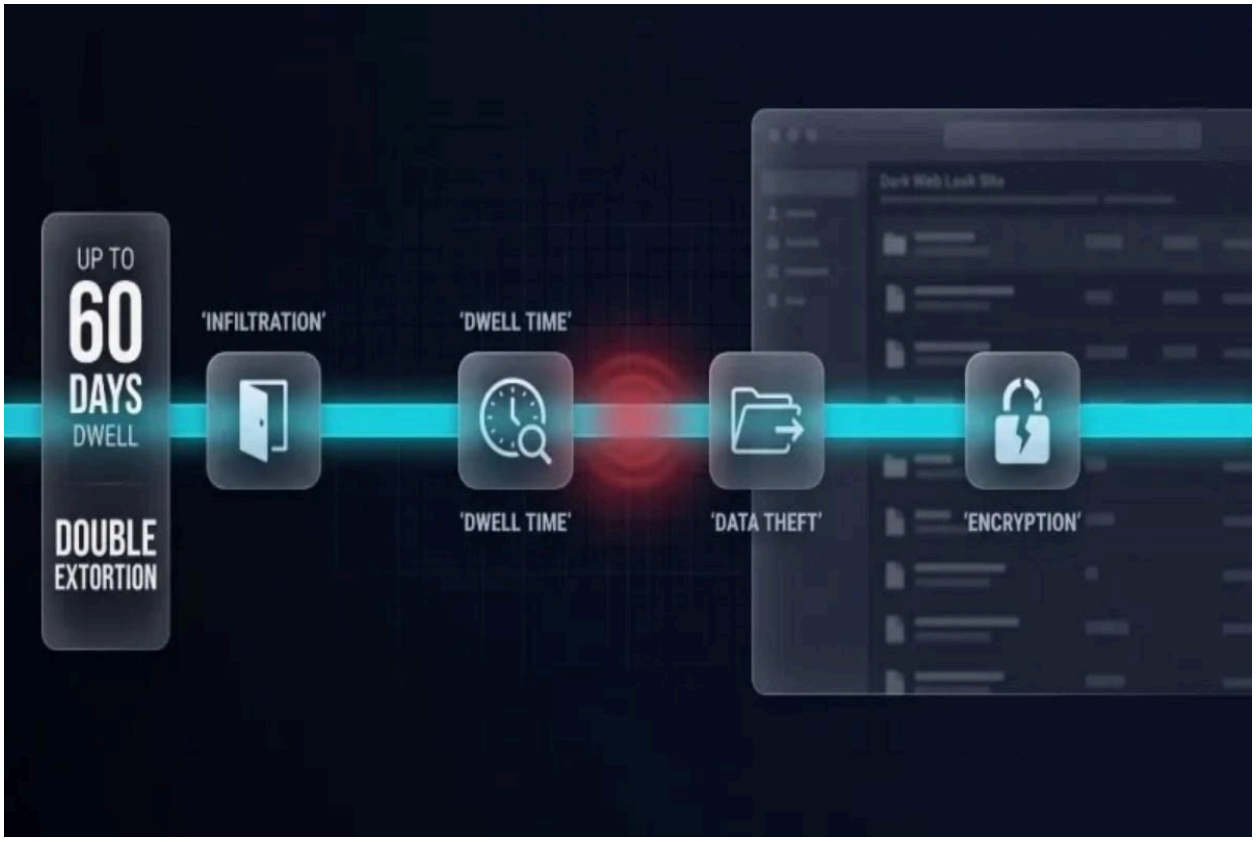
Initial Access and Lateral Movement

Reporting notes that the group has targeted managed service providers and remote-management tooling to reach many downstream organisations at once. Sophos reported in 2025 that flaws in the SimpleHelp remote-support software were abused in an attack on one such provider, which then exposed that provider's customers. After entry, attackers typically move laterally, escalate privileges, and disable backups before they deploy the encryptor. Ransomnews

Encryption and Extortion

Once the payload runs, files are locked and a ransom note directs the victim to a private negotiation portal. If talks stall, the stolen data may be posted on the leak site, which puts public pressure on the victim's customers, partners, and regulators. The group publicly says it avoids

healthcare targets, but that is a criminal marketing claim and should never be treated as protection. Ransomnews



Scale and Trends: What the Numbers Say

Leak-site tracking shows 101 new victims in the first quarter of 2026, a 29 percent jump from the previous quarter, and the cumulative total reached 645 by the end of August. Another tracker reported a quieter second quarter of roughly 27 victims, which shows that criminal activity moves in waves and not in a straight line. Industry breakdowns list professional services at 23 percent, manufacturing at 22 percent, and technology at 12 percent of known victims. Because these counts come from the criminals' own postings, they are useful for spotting trends but should not be read as exact measures of total infections. DragonForce Ransomware | Group Profile & Attack Analysis +2

Industries at Risk

Professional services, manufacturing, and technology firms appear most often, likely because they hold valuable data and cannot tolerate long downtime. Postings from June 2026 included a Swedish steel manufacturer, a Hong Kong shipyard and serviced-apartment complex, and a construction firm in the UAE. The message for students is that no sector is too small or too obscure to be a target. Breached

Why Trackers Disagree

Different trackers count at different times, use different definitions of a "victim", and sometimes double-count rebranded or reposted entries. For example, one vendor summary counted 253 claimed victims in the first half of 2026, while other sources reported far lower quarterly totals. When you cite ransomware statistics, always name the tracker and the date, and treat every number as an approximation.

Protecting Your Organisation: Practical Defences

Good defence starts with the basics that agencies such as CISA and the FBI repeatedly recommend in their joint #StopRansomware guidance. Strong identity controls, tested backups, and fast patching remove the easiest routes that affiliates rely on. Adding **Digital risk protection** to your security programme helps you spot leaked credentials, brand impersonation, and stolen-data postings before they grow into a full crisis. The checklist below turns these ideas into actions that even a small team can begin this week.

- Enforce phishing-resistant multi-factor authentication on email, VPN, and admin accounts.
- Verify caller identity before any help-desk password or MFA reset.
- Patch internet-facing systems and remote-management tools promptly.
- Keep offline, immutable backups and test a restore every quarter.
- Segment your network so one infected device cannot reach everything.
- Use endpoint detection and response with round-the-clock monitoring.
- Review vendor and MSP access, and remove unused remote-support software.
- Train staff to recognise phishing emails and voice-phishing calls.

Build and Rehearse a Recovery Plan

A backup that has never been restored is only a hope, so schedule realistic restore drills that measure how long critical systems take to return. Write down who makes decisions, who speaks to customers, and how the business will operate manually if computers are unavailable. Rehearsing with a tabletop exercise once or twice a year turns a panicked improvisation into a calm, practised routine.

Responding to an Incident: What to Do First

If ransomware strikes, speed and calm matter more than perfection. Isolate affected machines from the network, but avoid powering them off blindly, because volatile memory can hold clues that investigators need. Contact your incident response team, cyber insurer, and legal counsel early, and report the crime to authorities such as the FBI, CISA, or the UK's National Cyber Security Centre. The steps below give you a simple order of operations.

- Disconnect infected devices and disable compromised accounts.
- Preserve logs, ransom notes, and forensic images before cleaning anything.

- Identify what data was taken, since notification laws may apply.
- Restore from clean backups only after the intruder's access is removed.
- Reset all credentials, including service accounts and API keys.
- Document every action for insurers, regulators, and lessons learned.

Should You Pay the Ransom?

Law enforcement agencies generally advise against paying, because payment does not guarantee the return of data and it funds further attacks. Payment can also create legal or sanctions risk depending on who is ultimately behind the operation. Any decision should be made with legal counsel, your insurer, and law enforcement guidance, never under pressure from a countdown timer.

Monitoring the Dark Web After an Incident

Attackers sometimes re-post or resell stolen data long after the first extortion attempt ends. Continuous **Digital risk protection** can watch leak sites, paste sites, and criminal forums for your company name, domains, and employee credentials. Early alerts give you time to warn affected customers, reset exposed passwords, and prepare a factual public statement.

Related Entities and Concepts: Connecting the Dots

To understand the topic fully, it helps to know the related names in the ecosystem. LockBit and Conti provided leaked code, the collapse of RansomHub in April 2025 sent tools and affiliates toward DragonForce, and Scattered Spider supplied social-engineering skill in the UK retail cases. Frameworks such as MITRE ATT&CK map these behaviours into techniques that defenders can detect, while CISA advisories translate them into practical guidance. Seeing the ecosystem as a web of linked entities, not a single villain, explains why takedowns are so difficult and why defenders must focus on behaviours and not only on brand names. DeXpose

Alliance with LockBit and Qilin

In 2025 the operators publicly announced a partnership with Qilin and LockBit to coordinate attacks, share resources, and reduce conflicts. Researchers stress that the **dragonforce ransomware group** and its partners remain separate organisations that keep their own leak sites, so the alliance is closer to a trade association than a merger. No confirmed takedown had occurred at the time of writing, so defenders should assume the operation remains active. BreachedDeXpose

Conclusion

DragonForce shows how ransomware has matured from lone hackers into a franchise-style industry with shared tools, affiliate brands, and even extortion "consulting". Its rise, its UK retail attacks, and its alliances teach the same lesson: attackers often succeed through people, remote-access tools, and weak recovery plans, not through magic. The good news is that

identity hardening, tested backups, vendor oversight, and continuous monitoring make an organisation a much harder and less rewarding target. Keep learning from reliable sources, verify statistics before you share them, and treat preparation as a routine habit and not a one-time project.

Frequently Asked Questions (FAQ)

Is DragonForce only a danger to large companies?

No, small and mid-sized businesses are also targeted, especially when they use managed service providers or exposed remote-access tools. Attackers often prefer organisations that cannot afford long downtime, whatever their size. Basic controls such as MFA, patching, and offline backups protect firms of every size.

Does DragonForce attack hospitals?

The group has publicly stated that it avoids healthcare targets. However, that statement comes from criminals, and affiliates using shared tools may not follow it. Healthcare organisations should therefore keep the same defences as any other sector.

Is DragonForce the same as LockBit or Qilin?

No, they are separate groups that announced a cartel-style alliance to share resources and affiliates. Each keeps its own brand, leak site, and operations. Think of them as competitors who agreed to cooperate on selected matters.

How can I check whether my company data has been leaked?

Start by monitoring leak sites, breach-notification services, and dark web sources for your domains and employee emails. Many security vendors offer continuous monitoring that alerts you when your name appears. If you find a match, involve your incident response team and legal counsel immediately.

What is double extortion?

Double extortion means criminals steal your data first and then encrypt your systems. Even if you restore from backups, they threaten to publish the stolen files unless you pay. This is why prevention and data protection matter as much as backups.