# DragonForce introduces white-label ransomware as a service with affiliate scheme



A ransomware group known as DragonForce has introduced a new business model in the cybercrime world by offering ransomware as a service (RaaS) with a white-label affiliate scheme. This development allows other cybercriminal groups to use DragonForce's ransomware infrastructure and malware while conducting attacks under their own branding. The change is part of DragonForce’s evolution towards a distributed, cooperative "cartel" model, which it announced in an underground post in March 2025. DragonForce first surfaced in August 2023.

Under this model, affiliates do not need to manage the technical components typical of ransomware operations. DragonForce will handle critical elements such as malware development, the negotiation sites for ransom discussions, and data leak platforms, which are hosted on the dark web via Tor-based ".onion" domains. Cybersecurity researchers from Secureworks detailed that the offered package includes administration and client panels, encryption and ransom negotiation tools, file storage systems, and dedicated support services, all designed to simplify ransomware attacks for affiliates.

This approach mirrors trends seen in other criminal enterprises such as drug cartels, where cooperation and distribution networks facilitate broader reach and operational efficiency. It aligns with ongoing trends in ransomware operations where ease of access and reduced technical barriers are expanding the pool of actors able to carry out attacks.

Another ransomware group, Anubis, which began operations in December 2024, has similarly launched an affiliate programme. This scheme offers an 80% cut of ransom payments to participating affiliates, further indicating a move towards commercial-style partnerships in cybercrime.

The exact number of affiliates leveraging these schemes remains unclear; however, reports from Bleeping Computer confirm that at least one group, RansomBay, has joined DragonForce’s affiliate programme.

Secureworks commented on the development, stating, "Cybercriminals are motivated by financial gain, so they are adopting innovative models and aggressive pressure tactics to shift the trend in their favour."

The Tech Radar article noted the increasing democratization of ransomware, likening it to how artificial intelligence has broadened access to programming. By lowering the technical threshold and bearing operational complexity, ransomware-as-a-service schemes empower less technically skilled threat actors to target victims more effectively.

Security experts continue to recommend measures to mitigate ransomware risks, including regularly updating internet-facing devices, using phishing-resistant multi-factor authentication, maintaining reliable backups, and monitoring networks for suspicious activities. These practices remain crucial as ransomware operations become more accessible to a wider range of criminals.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.bleepingcomputer.com/news/security/dragonforce-expands-ransomware-model-with-white-label-branding-scheme/> - This article provides details on DragonForce's white-label affiliate model, explaining how it allows affiliates to use DragonForce's infrastructure while branding their attacks under their own names. It also mentions that DragonForce handles critical components such as malware development and negotiation sites.
2. <https://www.techradar.com/pro/security/dragonforce-ransomware-group-evolves-new-cartel-business-model> - This Tech Radar piece describes DragonForce's new business model, comparing it to a cartel structure and noting how the group offers a full suite of services including administration panels, encryption tools, and data leak sites. It highlights the democratization effect similar to AI's influence.
3. <https://www.broadcom.com/support/security-center/protection-bulletin/dragonforce-ransomware-s-campaign-intensifies-in-2025> - This Broadcom article mentions DragonForce ransomware's increased activity, although it does not specifically address the new business model. It provides context on the group's escalation and victim count.
4. <https://therecord.media/ransomware-groups-test-new-business-models-dragonforce-anubis> - This record.media piece discusses how DragonForce and Anubis are adopting affiliate models to entice hackers, reflecting a shift towards commercial partnerships in cybercrime.
5. <https://www.secureworks.com/blog/ransomware-groups-evolve-affiliate-models> - Secureworks details the evolution of ransomware affiliate models, highlighting DragonForce's novel approach. They describe features such as client panels and support services designed to facilitate attacks for affiliates.
6. <https://www.noahwire.com> - The source article discusses DragonForce's new RaaS model, its impact on criminal enterprises, and the democratization of ransomware. However, since the article's content is not accessible, it cannot be directly corroborated.
7. <https://www.techradar.com/pro/security/dragonforce-ransomware-group-evolves-new-cartel-business-model> - Please view link - unable to able to access data