DRAGONFORCE

[/ 'dreg.ɪn fors /]

DragonForce, a Malaysia-based group active since 2023, shifted from hacktivism to ransomware for financial gain. Known as “DragonForce Malaysia,” it runs the RansomBay extortion service and develops custom ransomware. Assessed as high risk, it targets government, retail, healthcare, tech, and utilities worldwide, with recent 2025 attacks on major UK retailers like Harrods and M\&S.

IDENTITY

Attribution	: DragonForce, first observed in August 2023, is a Malaysia-based group. Initially identified as a pro-Palestinian hacktivist collective, it has since evolved into a financially motivated ransomware operation.
Active Since	: August 2023
Aliases	: “DragonForce Malaysia”; operates the RansomBay white-label extortion service.
Motivation	: Transitioned from ideological hacktivism to multi-extortion financial gain.

TTPs

Initial Access	: Exploitation of internet-facing vulnerabilities; phishing campaigns.
Persistence	: Deployment of custom ransomware payloads across Windows, Linux, ESXi, and NAS platforms.
C2 Infrastructure	: Uses TOR-based leak sites and RansomBay extortion platform.
Malware & Tools	: Custom ransomware derived from Conti v3 codebase, initially linked to LockBit/Bilk sources.
Techniques	: Multi-extortion (encryption, data exfiltration, publication threats). Expansion into “Ransomware-as-a-Service” (RaaS) with RansomBay.

TARGET PROFILE

Target Sectors	: Government institutions, retail companies, legal firms, healthcare providers, technology firms, utilities.
Geographies Targeted	: Global focus; primary activity in UK, Israel, India, Saudi Arabia, Australia, with origins in Malaysia.

THREAT ASSESSMENT

Risk Level	: High — demonstrated ability to conduct impactful operations across diverse industries.
Most Recent Activity	: High-profile ransomware campaigns in April–May 2025 targeting UK retail giants (Harrods, Marks & Spencer, Co-Op).
Evolution	: Shift from hacktivist operations to full-scale financial ransomware campaigns. Development of multi-platform ransomware variants and the launch of RansomBay, enabling third-party operators to leverage their infrastructure.

NOTABLE OPERATIONS

- **2023:** Initial emergence as DragonForce Malaysia, targeting Israel with hacktivist-style attacks.
- **- 2024:** Transition to ransomware operations, linked to attacks on government and corporate entities in Asia-Pacific.
- **- 2025 (Early):** Launch of RansomBay white-label service, expanding operations into RaaS.
- **- 2025 (Q2):** Major ransomware attacks on UK retail sector including Harrods, Marks & Spencer, and Co-Op, disrupting operations and drawing global attention.