Cyber Insight

DragonForce Group

Cyber Intelligence Bureau

a division of Epidemiology Labs

Cyberdefense

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Credits Orange Cyberdefense

Methods & Neutrality

The information in this document is the result of OSINT (Open Source Intelligence) investigations. These sources are of cyber origin, i.e. from open sources.

The sources have been correlated, validated and qualified as trusted sources.
This information is analysis from a strictly cyber perspective.

The whole report strictly respects the principle of neutrality, which is fundamental to the research carried out.

DragonForce Group

- **Creation date:** The hacktivist group DragonForce, also known as DragonForce Malaysia, emerged in August 2023, based in Malaysia, with an initial pro-Palestinian orientation. It formed alliances with groups such as T3 Dimention Team, Syntax Brute Code (SBC) Malaysia, and PANOC Team for campaigns like #OpsBedil, primarily targeting entities in Israel, India, and the United Kingdom. Over time, DragonForce evolved from a hacktivist group into a ransomware operation focused on financial gain, using payloads derived from LockBit and Conti, while still maintaining political motivations and launching attacks worldwide.

- **Probable Origin**: DragonForce was initially identified as a pro-Palestinian group based in Malaysia. Our sources indicate that Malaysia serves as the group's operational base. One reason cited for this choice is that the country may offer a relatively lax legal framework when it comes to cybercrime.

- **Main strategies:** The main attack strategies of DragonForce rely on their white-label Ransomware-as-a-Service (RaaS) cartel model to conduct extortion operations. Their key tools and services include customizable ransomware kits, a Tor-based infrastructure for leak sites such as "DragonLeaks," and centralized administration panels to oversee operations

- **Geopolitical Motivation:** DragonForce's main geopolitical motivations have historically been tied to supporting the Palestinian cause and opposing Israel and its diplomatic allies. Although the group has largely shifted toward financial objectives, this hacktivist background continues to influence the targeting of certain government and strategic entities, particularly in Israel and in countries considered adversaries.

- **Targeted business sectors:** The sectors most frequently targeted by the DragonForce group are primarily retail, government institutions, and a wide range of private companies that hold sensitive data, including those in finance, technology, and critical infrastructure. However, they tend to partially avoid certain healthcare organizations.

Identification

DragonForce has evolved from a pro-Palestinian hacktivist group based in Malaysia into a major player in organized cybercrime, now operating as a ransomware cartel using a Ransomware-as-a-Service (RaaS) model since 2023-2024. Their main objective is now financial extortion through double extortion tactics and selling their services, actively targeting a wide range of sectors and countries worldwide. The group employs custom malware, dark web leak platforms, and sophisticated psychological manipulation, while notably claiming to have a "moral compass" by avoiding attacks on certain healthcare institutions.

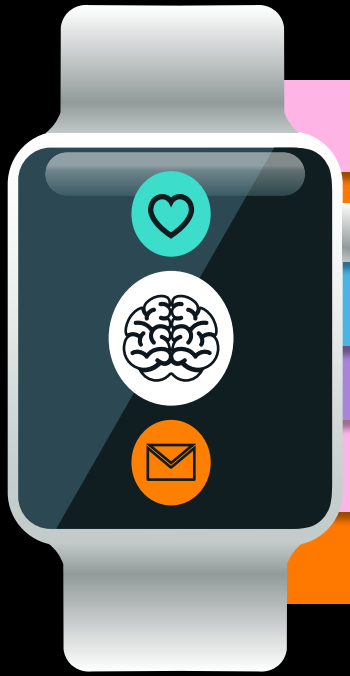
Credits Orange Cyberdefense

DragonForce Group: Main collaborating

Hacktivist Group Names

- RansomBay
- RansomHub
- T3 Dimension Team
- ReliksCrew
- KillNet
- Anonymous Sudan
- BlackLock
- Syntax Brute Code (SBC) Malaysia
- PANOC Team
- RAMP

Key Points



1
2
3
4
5
6

Structure

DragonForce primarily operates as a Ransomware-as-a-Service cartel using a white-label model.

Platform

A central team supplies the technical infrastructure, tools, and operational oversight, while affiliates carry out the attacks and share a percentage of the ransom payments collected.

Financing

DragonForce funds itself by taking a 20% share of ransom payments and also earns from selling stolen data and charging affiliates for access and subscriptions

Associated projects/tools

DragonForce focuses its technical development on offering a sophisticated white-label Ransomware-as-a-Service platform for affiliates, featuring customizable ransomware kits often built from leaked code like LockBit and Conti

Motivations

DragonForce's motivations have shifted from early hacktivism to mainly pursuing financial gain through its Ransomware-as-a-Service (RaaS) operations, although some ideological ties still remain.

Targets

The group's targets, which include government institutions and various private companies holding sensitive data, are increasingly focused on the retail sector for financial gain.

Vectors of Influence

1

Ideological Veneer

The group maintains a residual political or ideological framing, tied to its hacktivist roots and anti-Israeli stance. Today, this mainly serves as a facade to attract certain affiliates or add a layer to their public image.

2

Reputation and Alliances

DragonForce actively builds its reputation within the cybercrime ecosystem by forming alliances and showcasing successful operations. This influences other groups and potential affiliates to collaborate or join their RaaS platform.

3

Technical RaaS Offering

Offering a sophisticated white-label Ransomware-as-a-Service (RaaS) platform, with customizable tools, infrastructure, and support, is a major influence vector for attracting affiliates seeking effective, ready-to-use cybercrime capabilities.

4

Social Engineering

The group uses tricks like phishing and exploiting trust to fool people into giving them access or making mistakes.

5

Psychological Extortion Tactics

DragonForce uses intense psychological pressure on victims, including artificial urgency with countdowns, instilling fear and shame through public data leaks, leveraging deepfakes, and sending deceptive communications to coerce ransom payments.

Credits Orange Cyberdefense

Emotional Intelligence

1

By manipulating cognitive biases such as confirmation bias, authority effect, and peer pressure, leaders reinforce adherence, reduce critical thinking, and create an environment of conformity where questioning is marginalized.

2

Emotional manipulation techniques rely on fear, shame, pride, or belonging to control and motivate members or victims: threats, public humiliation, internal recognition. Everything is used to condition reactions.

3

DargonForce employs behavioral conditioning. By using positive reinforcement (such as rewards and recognition) and negative reinforcement (like exclusion and threats), the group effectively shapes its members' behaviors over time, relying on the principles of operant conditioning and social learning.

4

Advanced influence and persuasion techniques, utilizing Cialdini's principles of persuasion (social proof, scarcity, commitment, and authority), legitimize the group's power, spark interest, and drive action, while also creating a sense of urgency and exclusivity.

5

DragonForce uses tactics such as the widespread dissemination of contradictory messages (flooding), simulated empathy (fake negotiations), and NLP techniques (anchoring, reframing, confusion patterns) to lower vigilance, manipulate perception, and push targets toward submission or collaboration.

6

DragonForce uses integration rituals, validation ceremonies, and ideological hybridization to build strong group cohesion and justify illegal actions as serving a higher cause. Public commitment and submission to authority further reinforce loyalty, obedience, and a lasting collective identity within the group.

Professional Sectors

List of targeted sectors

- Government institutions
- Critical Infrastructure
- Private Companies
- Architecture and Engineering (A&E)
- Retail
- River Logistics
- Technology and IT Services
- Manufacturing and Industry
- Finance and Insurance
- Education
- Hospitality and Tourism
- Energy and Utilities
- Transport and Communications

Note

DragonForce represents a new generation of cybercriminal groups that blend political activism, advanced technologies, and profitable business models. Their shift from pure hacktivism to organized cybercrime signals a troubling trend, making global cooperation, stronger protections, and increased awareness essential to counter this emerging threat.

Targeted Countries

Australia
Singapore
Saudi Arabia
Israel
Europe
France
United Kingdom
Middle East
Asia
North America
Malaysia
India
United States
Italy
Canada

Credits Orange Cyberdefense

Most Likely Hypothesis

Strategic Targeting:
- DragonForce, now a financially motivated cybercriminal cartel, sees Europe as a lucrative target, focusing on high-value sectors like retail, government, critical infrastructure, finance, and technology. Their operations have already impacted the UK and Italy, with France likely at risk.

Hybrid Attack Methods:
- Their attacks combine advanced ransomware tools (RaaS) with psychological manipulation, using phishing, AI-driven personalization, and leaked ransomware kits for technical access, while applying pressure tactics like strict payment deadlines and public data leaks to maximize impact and ransom payments.

Systemic Impact:
- A major DragonForce attack could cause widespread operational disruption, financial losses, and reputational damage across Europe's critical sectors. Their decentralized affiliate model enables simultaneous, hard-to-trace attacks, increasing systemic risk and challenging defense efforts.

Credits Orange Cyberdefense

The most dangerous hypothesis

Feared Scenario:
- Coordinated large-scale attack against European critical infrastructure (energy, transportation, telecom, gov), combining ransomware, data extortion, and sabotage, orchestrated through an affiliate model and automated (AI-driven) tools.

Primary Targets:
- High-impact sectors (telecom, energy, transportation) to maximize disruption and media attention.

Methodologies:
- Phishing, exploitation of vulnerabilities, stealthy lateral movement (LOTL).
- Use of modular ransomware (LockBit 3.0, RansomHub) and data exfiltration tools.
- Automation and customization of attacks via AI and affiliate model.

Potential Consequences:
- Massive shutdowns of essential services, major economic losses.
- Amplified chaos, loss of public trust, increased pressure on European cybersecurity.

Credits Orange Cyberdefense

Cyber Intelligence Bureau

a division of Epidemiology Labs

Build a safer digital society

Cyberdefense

https://www.orangecyberdefense.com/global/insights/research-intelligence/epidemiology-labs

Credits Orange Cyberdefense