DRAGONFORCE AND ANUBIS RANSOMWARE OPERATORS INTRODUCE NEW AFFILIATE MODELS

Vairav Cyber Security Campaign Report

Date: April 28, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

In 2025, ransomware groups continue to adapt despite intensified global law enforcement efforts. DragonForce and Anubis ransomware operators have unveiled new affiliate models to expand their operations and maximize profits. DragonForce has rebranded itself as a "cartel," offering affiliates the ability to build personalized ransomware brands. Meanwhile, Anubis has introduced a three-tiered extortion system that includes encryption, pure data theft, and monetization of unauthorized access, highlighting an alarming evolution in extortion techniques.

INCIDENT DETAILS

DragonForce, active since August 2023, transitioned from a traditional Ransomware-as-a-Service (RaaS) model to a decentralized cartel structure by early 2025. Affiliates can now create their own ransomware brands while utilizing DragonForce's robust infrastructure. As of March 2025, DragonForce had listed 136 victims on its leak site.

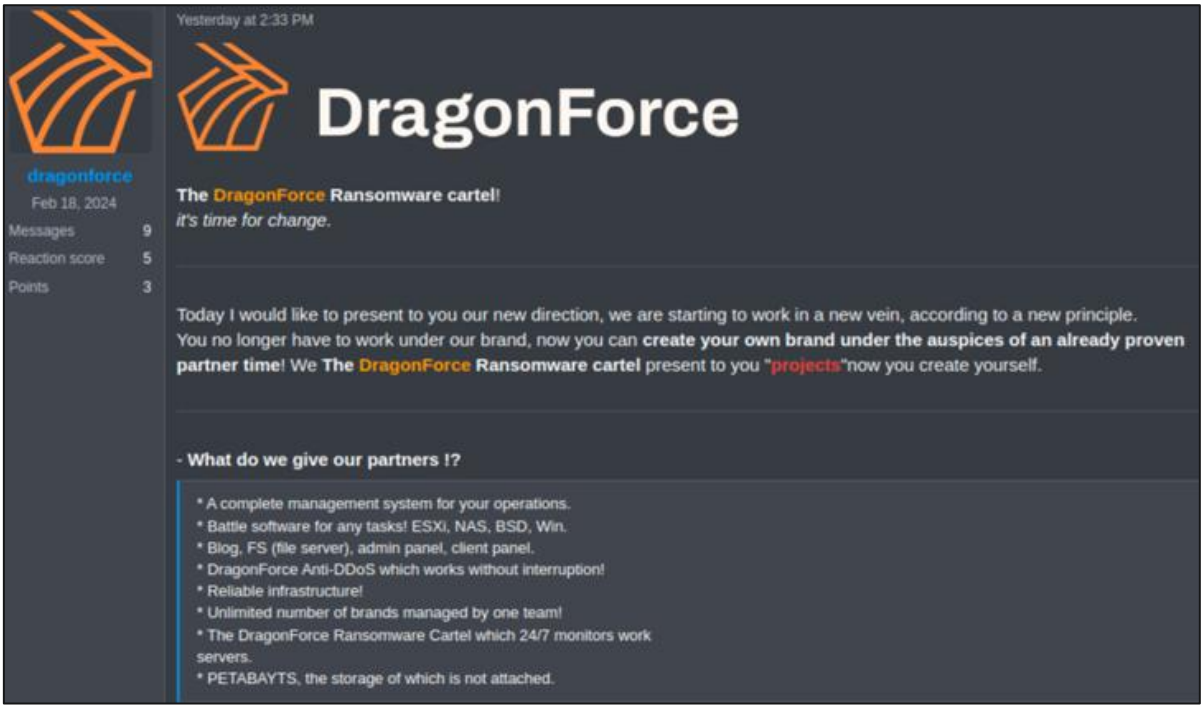

Figure 1: DragonForce announcement about the shift to a customizable affiliate model.

Anubis, emerging in February 2025, has disrupted the conventional ransomware model by offering three operational modes:

- **File Encryption:** Standard ransomware attacks with affiliates earning 80% of ransom payments.
- **Data Ransom:** Focused exclusively on data exfiltration and blackmail without encryption, offering affiliates 60%.
- **Accesses Monetization:** Assisting affiliates in extorting ransoms from compromised networks, providing a 50% cut.

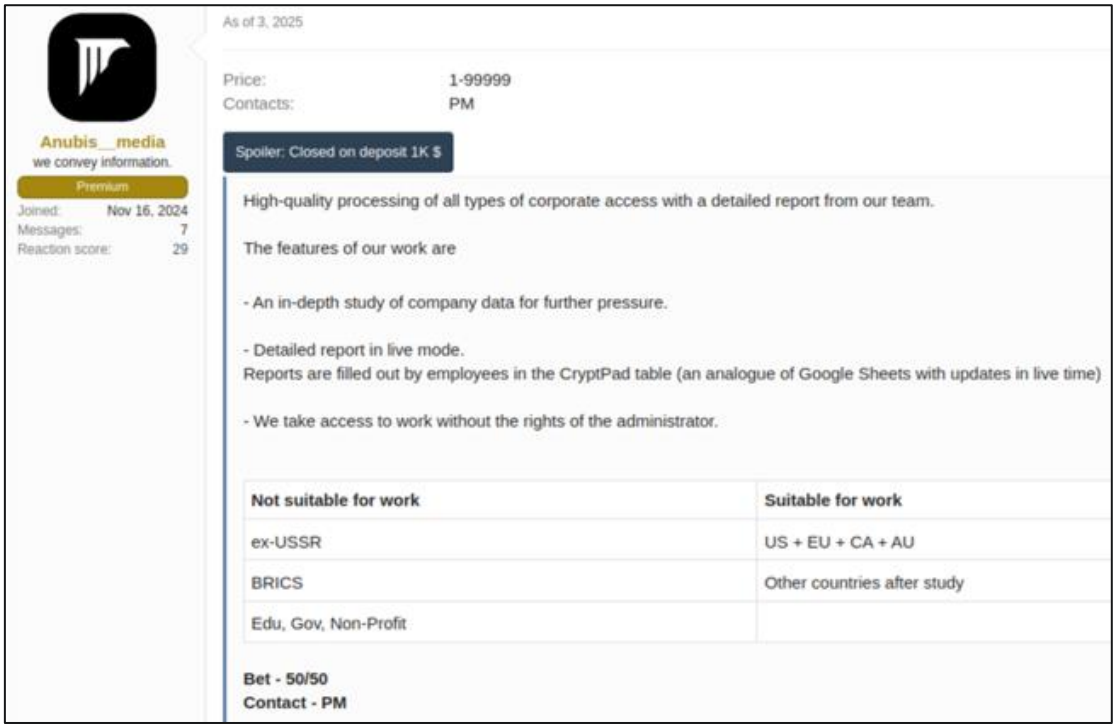

Figure 2: Advertisement for Anubis "accesses monetization" service

Notably, Anubis leverages psychological pressure tactics, threatening non-paying victims with public exposure on social media platforms and regulatory reporting to authorities like the UK ICO and the US Department of Health and Human Services. This mirrors tactics first seen with groups like ALPHV (BlackCat) in late 2023. These new business models illustrate the increasing commercialization and diversification of ransomware activities, making it even harder for organizations to defend against and recover from attacks.

RECOMMENDED ACTIONS

- **Enhance Incident Response Plans:** Update playbooks to account for data theft-only scenarios and regulatory extortion threats.
- **Implement Strong Backup Strategies:** Maintain offline and immutable backups to reduce leverage from ransomware encryption.

- **Monitor for Unauthorized Access:** Proactively detect and investigate unusual access attempts to prevent initial breaches.
- **Strengthen Cyber Insurance Policies:** Ensure cyber insurance covers data breach notification and regulatory fine risks.
- **Educate Employees:** Conduct regular phishing and social engineering training to reduce the likelihood of initial compromise.
- **Adopt Zero Trust Principles:** Limit lateral movement across networks to contain potential attacks.

ADDITIONAL RESOURCES

https://www.secureworks.com/blog/ransomware-groups-evolve-affiliate-models

https://cybersecuritynews.com/dragonforce-and-anubis-ransomware-operators/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com