TIR-20250716 DragonForce Ransomware

7/16/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary 3
DragonForce Ransomware 4
Tactics and Techniques 4
Recent Attacks 6
Conclusion 7
MITRE MAP 8
Aspire Protects 9
Indicators of Compromise (IoCs) 10
Supporting Documentation 11
Appendix II: Disclaimer 12

Executive Summary

DragonForce is a relatively new but fast-growing ransomware-as-a-service (RaaS) operation that has made its presence known through disruptive attacks and bold extortion campaigns. Since its emergence in late 2023, the group has repeatedly targeted high-profile organizations across the retail, education, healthcare, and government sectors. Unlike other structured and disciplined ransomware groups, DragonForce enjoys chaos and public pressure tactics - often choosing visibility and political impact over negotiation. Their attacks typically follow a double-extortion model and are frequently accompanied by large data leaks and messaging via their Tor-based leak site and Telegram channels.

The group made headlines in early 2024 after concurrent attacks on the government of Palau and private corporations across multiple continents. In one of the more chaotic episodes, DragonForce and LockBit both claimed responsibility for the Palau incident, leading to confusion and conflicting ransom instructions. More recently, DragonForce claimed responsibility for a May 2025 attack on U.S. retailer Belk, which resulted in the theft of 156GB of data, including personally identifiable information (PII) such as names and Social Security numbers.

DragonForce's evolution from political hacktivism to commercial ransomware has made it an unpredictable threat actor. The group is actively expanding its affiliate base, recruiting pentesters and access brokers, and offering a cut of 80% to partners. Their

ransomware payloads are customizable, with options to tailor encryption behaviors and impersonation tactics - many of which borrow heavily from leaked LockBit Black code.

DragonForce Ransomware

The origins of DragonForce can be traced back to 2021, when a Malaysian hacktivist group using the same name launched a wave of politically motivated cyberattacks against government and private sector targets across Asia and the Middle East. While it remains unclear whether the current ransomware operation is a direct continuation of the original DragonForce hacktivist crew, the group has adopted similar branding, tactics, and ideological messaging.

In November 2023, DragonForce ransomware first appeared in the wild, with attacks against Yakult Australia, Coca-Cola Singapore, and the Ohio Lottery marking their debut. These incidents showed a clear escalation in both capability and intent, as the group shifted from simple defacements to full-on ransomware operations involving data exfiltration and encryption.

DragonForce runs a white-label RaaS model, providing affiliates with access to a full-featured control panel, automated payload builders, and revenue-sharing agreements. Their infrastructure allows for targeting across Windows, Linux, ESXi, and NAS environments. Encryption techniques include AES-256 and RSA, with newer versions incorporating ChaCha8 for faster performance. Despite these capabilities, the group continues to show signs of operational immaturity, including sloppily written ransom notes, inconsistent encryption outcomes, and overlapping claims with other ransomware groups.

Tactics and Techniques

DragonForce ransomware attacks follow a familiar lifecycle, but with several unique twists. Initial access is most often achieved via phishing emails, brute-force attacks on exposed RDP or VPN services, or exploitation of known vulnerabilities. CVEs like

Log4Shell (CVE-2021-44228) remain part of their playbook, particularly in under-resourced environments.

Once inside the network, DragonForce operators deploy a mix of commodity and open-source tools to facilitate lateral movement, data collection, and eventual encryption. Tools like Mimikatz and Cobalt Strike are commonly observed, alongside less sophisticated methods like token impersonation and use of stolen credentials. Persistence is often achieved through registry run keys or the deployment of remote access software.

DragonForce practices dual extortion. This means that they encrypt systems and exfiltrate sensitive data for later publication. Leaks are published on their dark web leak site, often alongside media files such as screenshots and audio recordings of ransom negotiations. In at least one case, they uploaded voice recordings of negotiations to apply psychological pressure on the victim.
Customization plays a large role in their tooling. Affiliates are provided with a configuration file ("config.json") to tailor behaviors such as encryption paths, language filters (e.g., avoid encrypting CIS countries), and ransom note content. This flexibility makes DragonForce a tempting platform for less experienced threat actors looking for turnkey ransomware deployment.

Links to Other Groups

DragonForce's use of the LockBit Black builder (originally leaked in September 2022) places them within a growing cluster of groups that rely on repurposed code from more sophisticated ransomware families. While there is no direct evidence of collaboration with LockBit, the technical similarities are significant, particularly in payload structure and configuration options.

DragonForce has also been linked to previous hacktivist collectives operating out of Malaysia and Indonesia. Their blend of ideological messaging and use of defacement tactics is consistent with the MO of Southeast Asian hacktivist crews active during 2021 - 2022. However, it remains unclear if the ransomware variant is run by the same individuals or merely inspired by the original group's brand and messaging.

Indirect connections to Scattered Spider have also been noted in some attacks, particularly those involving large retail brands in the UK. While attribution remains unclear, shared TTPs and overlapping victim profiles suggest either coordination or

imitation. The use of Telegram for recruitment and propaganda mirrors tactics seen from other politically motivated ransomware groups like SiegedSec.

DEVMAN – A Variant of DragonForce

DEVMAN ransomware is widely considered a spinoff of DragonForce, built on the same foundational codebase but exhibiting distinct characteristics. While antivirus engines often label DEVMAN samples as DragonForce or Conti variants, DEVMAN introduces subtle but telling changes. Most notable change is the use of a .DEVMAN file extension and a malfunctioning builder that encrypts its own ransom notes. Despite these differences, DEVMAN still drops DragonForce-branded ransom notes, which likely means DEVMAN is reusing DragonForce's infrastructure or tooling, likely through the group's Ransomware-as-a-Service (RaaS) program. Affiliates appear to be customizing payloads with minimal effort, leading to operational overlap and confusion in attribution.

DEVMAN's operations are mostly offline, with no observed C2 communications, and include features like SMB probing, file scrambling and multiple encryption modes (including header-only and full encryption). The malware also leverages Windows Restart Manager for persistence and file lock bypass, mirroring techniques seen in both Conti and DragonForce. DEVMAN's dedicated leak site (DEVMAN's Place) has listed nearly 40 victims, primarily in Asia and Africa.

Recent Attacks

May 8–11, 2025

DragonForce compromised the systems of Belk, a major U.S. department store chain, stealing over 156GB of sensitive data. The attack forced Belk to shut down online operations and rebuild affected systems. Affected individuals were notified that names and Social Security numbers were exposed. DragonForce later published the stolen data on their leak site, indicating Belk did not pay the ransom.

March 2024

DragonForce and LockBit both claimed responsibility for encrypting systems belonging to the Palauan government. Conflicting ransom instructions were issued, creating

confusion. Palauan officials denied paying or engaging either group. This incident suggested potential internal disorder among cybercriminal affiliates.

November 2023

DragonForce targeted the Aussizz Group, a prominent educational and migration consultancy, claiming to exfiltrate and encrypt nearly 300GB of sensitive data. Public exposure of data has not yet been confirmed, but the incident established the group's capability to impact large organizations.

January–April, 2025

DragonForce has taken responsibility for attacks on major UK retailers including Co-op, Harrods, and Marks & Spencer. These incidents resulted in system outages and operational disruption. Some attacks have also been linked to the Scattered Spider threat actor, raising questions about coordination or false flag operations.

CONCLUSION

DragonForce started with hacktivist roots but has shifted into a messy, money-driven ransomware operation. What makes them threatening isn't technical sophistication, it's how easy they've made it for others to join in. By using leaked tools and pressuring victims, they've lowered the bar for entry while increasing the damage they can cause. For organizations without strong defenses, that's a bad combination.

From a CTI perspective, DragonForce's value lies not just in their technical profile but in what they reveal about the current ransomware ecosystem. They make it clear that the current ransomware landscape is noisy. DragonForce is not the most advanced group, but they don't need to be. Their unpredictability and willingness to leak sensitive data even in low-value campaigns make them a persistent threat.

ASPIRE'S RECOMMENDATIONS

Organizations should take the following actions to protect against DragonForce ransomware:

- Conduct immediate audits of public-facing applications, VPNs, and remote access points. Patch or disable vulnerable services.
- Apply geo-blocking rules where possible, particularly for traffic originating from Southeast Asia if not business-critical.
- Strengthen email defenses to catch phishing lures often used for initial access. Implement attachment and link scanning.
- Disable RDP where feasible. Require MFA for all remote access, including administrative logins.
- Review endpoint telemetry for signs of credential harvesting (e.g., Mimikatz) or the presence of tools like Cobalt Strike and ScreenConnect.
- Monitor defacement indicators, including file replacements and unauthorized web uploads.
- Build out an incident response plan that accounts for both encryption events and public exposure of sensitive data.

MITRE MAP

Initial Access	T1190 – Exploit Public Facing Application T1133 – External Remote Services
Execution	T1059 – Command and Scripting Interpreter T1059.003 – Command and Scripting Interpreter: Windows Command Shell
Persistence	T1219 – Remote Access Software T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Privilege Escalation	T1003.001 – OS Credential Dumping: LSASS Memory
Defense Evasion	T1562 – Impair Defenses T1218 – Signed Binary Proxy Execution
Exfiltration	T1041 – Exfiltration Over C2 Channel T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage
Impact	T1486 – Data Encrypted for Impact T1490 – Inhibit System Recovery

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

DragonForce

CVEs

- CVE-2024-21412
- CVE-2024-21887
- CVE-2024-21893

MD5

- 3c311cabe7de6a8c104f8f10541d392d
- 40126b1b3c6f86194fc554cdba3cb5d3
- cbcb58ffe45c202c11bcf2070496aed6
- d44071f255785c73909d64f824331ebf
- e4a4fc96188310b7b07e7c0525b5c0aa

SHA1

- 577b110a8bfa6526b21bb728e14bd6494dc67f71
- 81185dd73f2e042a947a1bf77f429de08778b6e9
- a05551c8536eb6489651a9481911d107fd1c34ef
- b47d1618177b6bc219b8734cd02f9cf7be7aff43
- f59f4be06c9d1a94d44d1f6a6afd4ad6d532cb47

SHA256

- 01f1e82d4c2b04a4652348fb18bb480396db2229c4fd22d2be1ea58e6bf4a570
- 312ca1a8e35dcf5b80b1526948bd1081fed2293b31d061635e9f048f3fe5eb83
- 5c54bd1aa2abf024f53490b7d93101496b5842a5a81a51955fe7f1d5e4281409

- 7126b9932dc0cdfe751340edfa7c4a14b69262eb1afd0530e6d1fdb2e25986dd
- 88169b1d4778ed6c5fda97375efb5b9171ea52649c8715bb449801c39bce4ad4
- ba1be94550898eedb10eb73cb5383a2d1050e96ec4df8e0bf680d3e76a9e2429
- d4de7d7990114c51056afeedb827d880549d5761aac6bdef0f14cb17c25103b3
- e1b147aa2efa6849743f570a3aca8390faf4b90aed490a5682816dd9ef10e473

DEVMAN

MD5

- e84270afa3030b48dc9e0c53a35c65aa

SHA1

- 4a34bbad85312ef34b60818a47f7b5bb8e9a7e26

SHA256

- 018494565257ef2b6a4e68f1c3e7573b87fc53bd5828c9c5127f31d37ea964f8
- df5ab9015833023a03f92a797e20196672c1d6525501a9f9a94a45b0904c7403

SUPPORTING DOCUMENTATION

DragonForce Ransomware | Intel 471

DragonForce: The Ransomware Cartel Guarding Its Burrow - LevelBlue - Open Threat Exchange

DragonForce Ransomware - Emerging Threat - 8 May 2025

DragonForce Ransomware Group | Group-IB Blog

DragonForce: The Ransomware Cartel Guarding Its Burrow

DragonForce Ransomware: Redefining Hybrid Extortion in 2025 - Check Point Blog

DragonForce Ransomware Strikes MSP in Supply Chain Attack

DEVMAN Ransomware: Analysis of New DragonForce Variant - LevelBlue - Open Threat Exchange

DragonForce Ransomware's Campaign Intensifies in 2025

DragonForce expands ransomware model with white-label branding scheme

Ransomware Groups Evolve Affiliate Models | Secureworks

DragonForce Ransomware Group: Tactics, Targets & Mitigation

3 Cyber Attacks in June 2025: Remcos, NetSupport RAT, and more

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.