Quorum Cyber

Threat Intelligence DragonForce Ransomware

TLP Status: CLEAR

Prepared by:

Intelligence Cut-off Date (ICoD): 12/05/2025 10:00 UTC

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version		Date	Summary of Changes
0.1	AM	05/05/2025	Initial Report Drafted
0.2	VM	05/05/2025	Review
0.3	AM	09/05/2025	Update
1.0	VM	12/05/2025	Review/Update
1.1	JA	15/05/2025	Final Review

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
-	-	-

DragonForce RaaS Group Profile

Overview

Name: DragonForce (also known as "DragonForce Malaysia" in its early hacktivist phase).

Type: Cybercriminal group operating a Ransomware-as-a-Service (RaaS) platform with hybrid motivations (financial gain and some residual hacktivist ideology).

Origin/Base: Initially based in Malaysia, with a global affiliate network. Emerged as a ransomware threat actor around mid-2023.

Motivation: Primarily financial (extortion through ransomware), while occasionally aligning with political or ideological causes (a legacy of its hacktivist roots). The group's evolution represents a hybrid threat – blending hacktivist-style targeting with profit-driven cybercrime.

Current Status: As of 2025, DragonForce is a mature RaaS operation counted among the notable ransomware threats globally[1]. It actively recruits affiliates worldwide and provides them with tools and infrastructure to conduct attacks. Recent high-profile campaigns (e.g. attacks on major UK retailers) have raised DragonForce's profile on the international stage[2].

2025 GROUP RESTRUCTURE

In March 2025, DragonForce announced the group was re-branding as a 'Cartel' in an underground forum post. The new structure allows affiliates to use DragonForce's infrastructure, including administrative and encryption tools, file hosting systems, and its Tor-based leak website, while still allowing affiliates to operate with other branded malware. This has likely been conducted to 'lower the bar of entry' for less sophisticated threat actors that lack the required infrastructure to conduct malicious attacks.

Group Background and Identity

DragonForce originally formed as a hacktivist collective (known as DragonForce Malaysia) around 2021-2022. The group gained notoriety through ideologically motivated cyber campaigns, often tied to anti-Israel and anti-Western causes. DragonForce Malaysia has spearheaded operations like #OpsBedil and #OpsBedilReloaded (targeting Israeli organisations) and #OpsPatuk (a campaign against Indian targets following political controversy). During this hacktivist phase, its tactics included website defacements, data leaks, and Distributed Denial-of-Service (DDoS) attacks.

By mid-2023, DragonForce underwent a significant transformation. While retaining its name and some of its original members, the group shifted from pure hacktivism to financially motivated cybercrime. August 2023 saw the emergence of DragonForce as a RaaS operation. This pivot did not completely erase its ideological leanings – the group initially portrayed itself as a pro-Palestinian "hacktivist-style" operation – but over time its goals expanded beyond politics. The modern DragonForce still occasionally targets governments or entities tied to political causes, but money has become the main driver. DragonForce's identity has evolved into a hybrid extortion group: part hacktivist and part profit-focused ransomware gang.

Notably, DragonForce's early hacktivist alliances and branding provided a springboard for its criminal endeavours. The group had worked alongside other Southeast Asian hacktivist outfits (e.g. T3 Dimension Team, ReliksCrew) during 2021-2022[3], building a reputation and community. These connections and the skills gave DragonForce a foundation to enter the

[1] https://blog.checkpoint.com/security/dragonforce-ransomware-redefining-hybrid-extortion-in-2025
[2] https://www.computerweekly.com/news/366623685/Chaos-spreads-at-Co-op-MS-following-DragonForce-attacks
[3] https://www.radware.com/security/ddos-knowledge-center/ddospedia/dragonforce-malaysia

ransomware scene with a ready pool of talent and a flair for publicity. Today, the group still references its roots in propaganda, but it operates with the professionalism and structure of a seasoned cybercrime cartel.

RaaS Operations Overview

DragonForce now functions as a RaaS platform, effectively acting as a "crimeware cartel" enabling other threat actors (affiliates) to carry out ransomware attacks using DragonForce's malware and infrastructure. The group formally launched an affiliate programme in mid-2024, advertising on underground forums that it offers 80% of ransom profits to affiliates (keeping 20% commission for itself)[4]. This revenue split is slightly more generous to affiliates than many competing RaaS programmes, making DragonForce an attractive option for would-be cybercriminal partners.

Affiliate Platform: DragonForce provides a web-based affiliate console that is feature-rich and user-friendly for cybercriminals. Through this panel, affiliates can generate custom ransomware builds, manage victims ("clients"), communicate with the DragonForce operators or team members, and oversee the status of attacks and payments. The panel includes modules for client tracking, an integrated chat for negotiations, a "builder" interface to compile ransomware payloads, and even a test-decryption function to prove to victims that it can decrypt files.

White-Label Ransomware: A distinguishing aspect of DragonForce's RaaS offering is its emphasis on white-label customisation. Affiliates are not forced to use DragonForce branding in their attacks; instead, they can create unique ransomware brands and even separate leak sites, all while using DragonForce's malware under the hood. In early 2025, DragonForce rolled out a service called RansomBay, which is essentially a template for leak sites and branding that affiliates can adopt for their own extortion campaigns. For an added fee, an affiliate can disguise the ransomware as a completely different strain (with custom names, logos, ransom note styles, and file extensions), making it harder for victims or law enforcement to immediately trace the attack back to DragonForce's platform. The RansomBay leak site service gives each affiliate a dedicated space (often unique .onion Tor site) to publish stolen data under their chosen brand, while DragonForce handles the backend. This approach allows DragonForce to expand its reach - effectively franchising its ransomware - without every attack being obviously attributed to DragonForce. It also appealed to criminals left adrift by the shutdown of some competing RaaS operations (for instance, DragonForce reportedly absorbed affiliates from the defunct RansomHub service in April 2025).

Technical Basis: Under the hood, the DragonForce ransomware initially borrowed code from existing notorious ransomware. Early in its operations, the group used payloads built from the leaked LockBit 3.0 (LockBit Black) builder. LockBit's code gave DragonForce a quick start with a proven encryption scheme. However, the group did not stop there. It soon developed its own "original" strain based on the leaked Conti v3 source code, incorporating custom improvements. As a result, DragonForce now supports multiple ransomware variants: one that is essentially a LockBit fork and another that is a modified Conti fork with enhancements for stealth and speed. Both variants achieve file encryption (using strong ciphers like AES, ChaCha, and RSA for key protection) and are delivered through the affiliate platform. The affiliates can choose which variant to deploy per victim.

Impact

DragonForce's operations have had significant impact on a range of victims across different countries. The consequences of their attacks include prolonged business disruption, sensitive data theft, financial losses, and reputational damage for victim organisations.

One of the most high-profile incidents attributed to DragonForce was a series of ransomware attacks against major UK retailers in April 2025. The group has claimed attacks against well-known companies including Marks & Spencer (M&S), Harrods, and the Co-operative Group (Co-op), causing chaos in their operations[5].

[4] https://blog.checkpoint.com/security/dragonforce-ransomware-redefining-hybrid-extortion-in-2025
[5] https://www.sentinelone.com/blog/dragonforce-ransomware-gang-from-hacktivists-to-high-street-extortionists/

Key Incidents

Target Organisation	What Happened	Impact
Marks & Spencer (2025)	DragonForce affiliates breached M&S systems, stole the NTDS.dit Active Directory file, and likely used this to escalate privileges across the network.	The incident caused major disruptions in sales and logistics, reportedly wiping off an estimated £500 million from the company's market value within a week.
Co-operative Group (2025)	Attackers encrypted internal systems and stole data, including customer loyalty records. Data was later leaked online.	Multiple services were suspended, and millions of customer records were compromised, leading to reputational damage and likely regulatory scrutiny.
Harrods (2025)	Harrods was hit in a coordinated ransomware campaign alongside other UK retailers, leading to data theft and system outages.	Short-term disruption to IT operations and customer services, with exposure of employee and customer data increasing legal and reputational risks.
Oahu Transit Services (2024)	DragonForce ransomware was deployed on systems used by Honolulu's public transport authority.	Transit operations were reportedly disrupted, with scheduling and fare systems affected, leading to public service interruptions.
Government of Palau (2024)	Ransomware attack compromised Palau's government infrastructure, likely through exploitation of exposed services or credentials.	Government services experienced outages and sensitive administrative data was exposed or encrypted, impacting public sector continuity.
Yakult Australia (2024)	Ransomware attack encrypted core operational data systems used in manufacturing and logistics.	Production and distribution processes were delayed, likely resulting in lost revenue and product shortages.
Coca-Cola Singapore (2024)	DragonForce affiliates targeted the Singapore branch of Coca-Cola, stealing corporate documents and sensitive data.	Possible exposure of internal communications and business plans; reputational damage and increased scrutiny from regulators.
Ohio Lottery (2024)	DragonForce affiliates breached the Ohio Lottery's IT environment, leading to suspected encryption and data exfiltration.	Public trust and operations affected, including delays in lottery services and potential leak of winner or employee information.

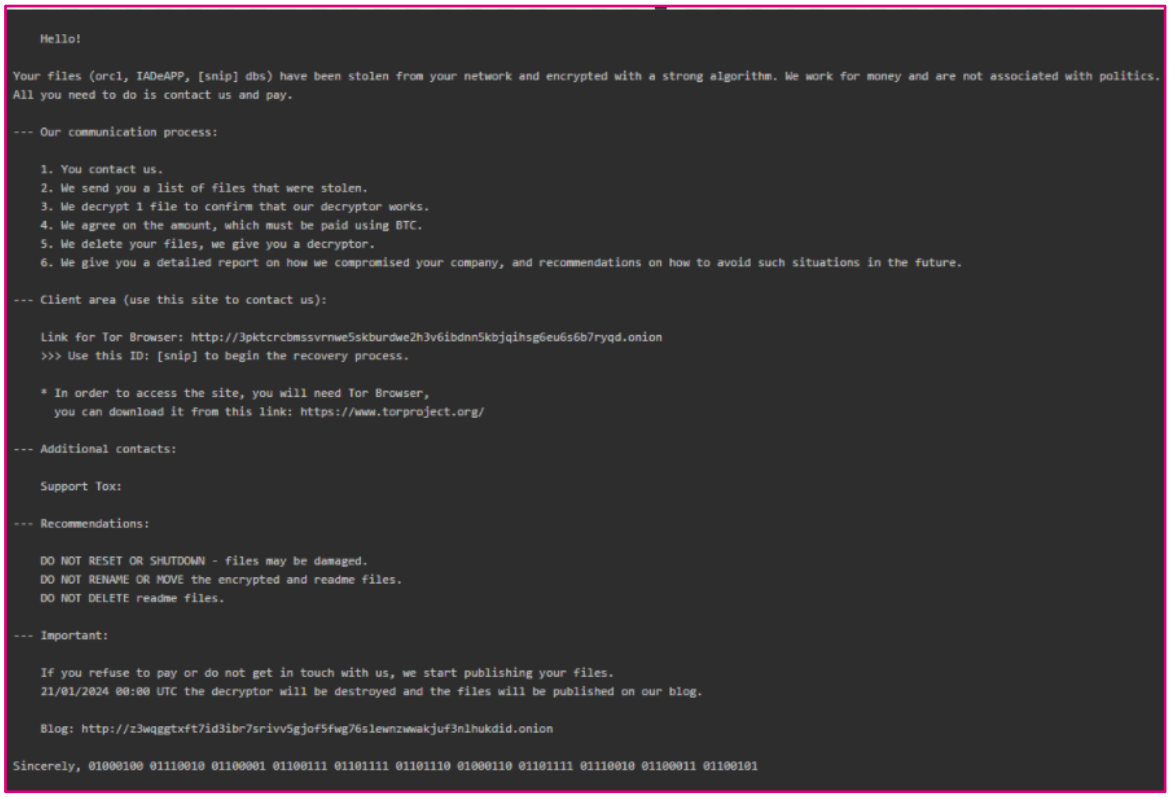
These examples demonstrate a global pattern of impact. Between August 2023 and August 2024, DragonForce claimed at least 82 victims on its dark web leak site[6]. Over half of those were organisations in the US, with others in the UK, Europe, Asia, and Australia. The industries affected range widely, but the consequences are consistently damaging: multi-million dollar losses from ransom payments or remediation, extended downtime (some victims experience weeks of disruption), and exposure of confidential or regulated data (leading to potential fines and lawsuits). Moreover, because DragonForce often threatens to leak stolen data (and follows through if unpaid), victims also suffer reputational harm when their

[6] https://medium.com/@tahirbalarabe2/the-rise-of-dragonforce-ransomware-ffc516836b32

breaches are publicised on leak sites and sometimes even on social media, given DragonForce's hacktivist streak in shaming targets.

Ransom Notes

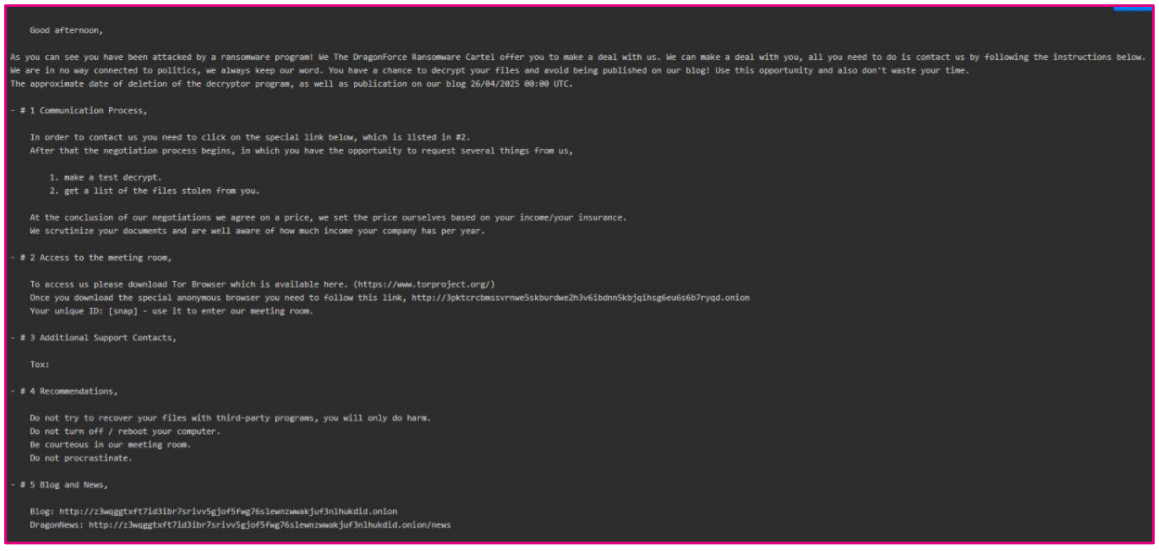
The ransom note appears as: **[rand].README.txt** (figure 1) and **README.txt** (figure 2)



```
    Hello!

Your files (orcl, IADeAPP, [snip] dbs) have been stolen from your network and encrypted with a strong algorithm. We work for money and are not associated with politics.
All you need to do is contact us and pay.

--- Our communication process:

    1. You contact us.
    2. We send you a list of files that were stolen.
    3. We decrypt 1 file to confirm that our decryptor works.
    4. We agree on the amount, which must be paid using BTC.
    5. We delete your files, we give you a decryptor.
    6. We give you a detailed report on how we compromised your company, and recommendations on how to avoid such situations in the future.

--- Client area (use this site to contact us):

    Link for Tor Browser: http://3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd.onion
    >>> Use this ID: [snip] to begin the recovery process.

    * In order to access the site, you will need Tor Browser,
      you can download it from this link: https://www.torproject.org/

--- Additional contacts:

    Support Tox:

--- Recommendations:

    DO NOT RESET OR SHUTDOWN - files may be damaged.
    DO NOT RENAME OR MOVE the encrypted and readme files.
    DO NOT DELETE readme files.

--- Important:

    If you refuse to pay or do not get in touch with us, we start publishing your files.
    21/01/2024 00:00 UTC the decryptor will be destroyed and the files will be published on our blog.

    Blog: http://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion

Sincerely, 01000100 01110010 01100001 01100111 01101111 01101110 01000110 01101111 01110010 01100011 01100101
```

Figure 1: DragonForce ransom note.

Source: Ransomware Live



```
    Good afternoon,

As you can see you have been attacked by a ransomware program! We The DragonForce Ransomware Cartel offer you to make a deal with us. We can make a deal with you, all you need to do is contact us by following the instructions below.
We are in no way connected to politics, we always keep our word. You have a chance to decrypt your files and avoid being published on our blog! Use this opportunity and also don't waste your time.
The approximate date of deletion of the decryptor program, as well as publication on our blog 26/04/2025 00:00 UTC.

- # 1 Communication Process,

    In order to contact us you need to click on the special link below, which is listed in #2.
    After that the negotiation process begins, in which you have the opportunity to request several things from us,

        1. make a test decrypt.
        2. get a list of the files stolen from you.

    At the conclusion of our negotiations we agree on a price, we set the price ourselves based on your income/your insurance.
    We scrutinize your documents and are well aware of how much income your company has per year.

- # 2 Access to the meeting room,

    To access us please download Tor Browser which is available here. (https://www.torproject.org/)
    Once you download the special anonymous browser you need to follow this link, http://3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd.onion
    Your unique ID: [snap] - use it to enter our meeting room.

- # 3 Additional Support Contacts,

    Tox:

- # 4 Recommendations,

    Do not try to recover your files with third-party programs, you will only do harm.
    Do not turn off / reboot your computer.
    Be courteous in our meeting room.
    Do not procrastinate.

- # 5 Blog and News,

    Blog: http://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion
    DragonNews: http://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion/news
```

Figure 2: DragonForce ransom note

Source: Ransomware Live

Data Leak Snapshot

Upon successful ransomware compromise, the DragonForce ransomware gang will upload victims to their **dark web leak site** (DLS), as shown in Figure 3. Victims can see their stolen data on the ransom site, which is typically accessed through a specific URL provided in the ransom note.

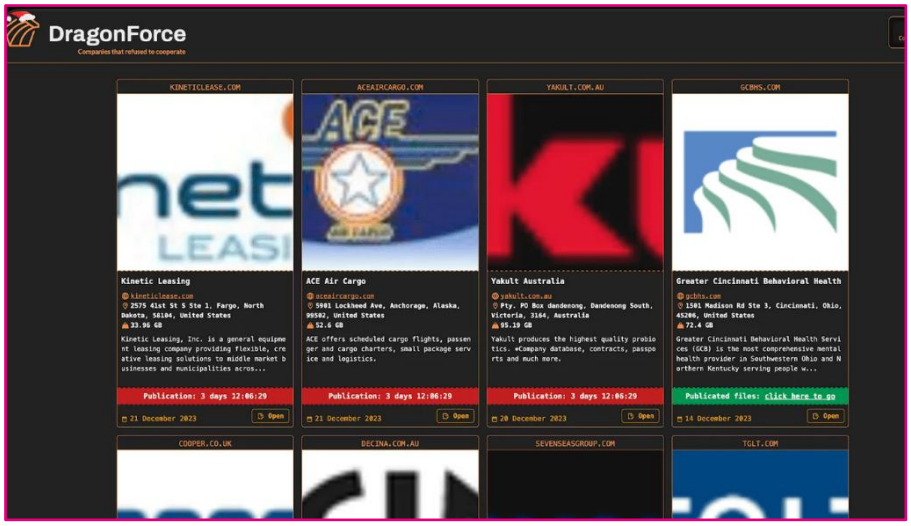


Figure 3: DragonForce ransomware leak site.

Data Source: Group-IB

Affiliates and Partnership

DragonForce's expansion and success are largely due to its affiliates. By design, the RaaS model means many of DragonForce's "operations" are actually carried out by these affiliates, who may have their own backgrounds and motivations.

Well-known ransomware groups who have had affiliations with DragonForce include:

- BlackLock
- RansomHub[7] (now absorbed by DragonForce)
- Scattered Spider[8].

Recruitment: DragonForce actively recruits a variety of cybercriminals, offering them tools and a profit share[9]. The recruitment posts on underground forums (like the RAMP forum on 26th June 2024) explicitly welcomed specialists such as "access brokers, pentesters, or pentesting teams" to collaborate. In these posts, DragonForce touted its advanced infrastructure and support, clearly positioning itself as a partner of choice for criminals looking to monetize their skills.

Notable Affiliate Groups: Recent investigations have revealed that certain high-profile hacking groups have acted as DragonForce affiliates. For example, the UK retail attacks in 2025 were eventually attributed to an affiliate group linked to the "Scattered Spider" and "The Com" collectives. Scattered Spider is an English-speaking group known for social

[7] RansomHub Went Dark April 1; Affiliates Fled to Qilin, DragonForce Claimed Control
[8] Scattered Spider Threat Actor Profile - Quorum Cyber
[9] https://www.group-ib.com/blog/dragonforce-ransomware

engineering and SIM-swapping attacks, and "The Com" is believed to be a loosely organised cybercriminal community. Its involvement suggests that DragonForce's affiliate pool now includes Western hackers who are highly skilled.

Hacktivist Collaborations: In its earlier incarnation, DragonForce Malaysia worked alongside other hacktivist groups (such as T3 Dimension Team and ReliksCrew) during campaigns like OpsBedil and OpsPatuk. Those weren't "affiliates" in the RaaS sense, but rather ideological partners. While DragonForce's current focus is profit, it's possible that some of those relationships persist in loose ways. DragonForce's operation today is run more like a business, so any ongoing hacktivist partnership would be opportunistic rather than formal. There is no clear evidence that the old hacktivist allies participate in the RaaS programme but, more likely, DragonForce's original members pivoted to crime and left purely ideological peers behind.

Targeted Sectors and Countries

DragonForce and its affiliates exhibit a broad targeting scope, which has expanded over time. Initially, as hacktivists, they focused on government and public sector targets tied to their causes. However, as a ransomware cartel, no industry is off-limits. Based on leaked victim lists and reporting from mid-2023 through 2024, the following sectors have been most impacted:

Targeted Sector	Analyst Comment
Manufacturing	The single most targeted industry by DragonForce in its first year of ransomware activity. About 14.6% of recorded DragonForce incidents hit manufacturing companies.
Real Estate	Real estate was the second-most attacked sector at ~13.4% of incidents.
Transportation	The third most affected sector (~12.2% of incidents).
Government and Public Sector	Government agencies (national and local) are frequent DragonForce targets, consistent with the group's hacktivist streak.
Retail	As evidenced by the 2025 UK retailer attacks, DragonForce is actively targeting the retail sector. Retail companies (supermarkets, chains, e-commerce) hold masses of customer data and rely on IT for sales which is a ripe target for double extortion.
Healthcare	Healthcare organisations, including clinics and hospitals, have been heavily targeted by DragonForce.
Legal Services	DragonForce is known to focus on law firms.

Geographically, DragonForce's reach is global. In the 82 victim cases observed in a 12-month period, roughly 52% were in the US, 12% in the UK, 6% in Australia, with the remaining 30% spread across regions including Asia (notably India, Malaysia, and Singapore), the Middle East (including Israel and Saudi Arabia), and smaller percentages in Europe and other locations.

Attack Lifecycle and Tradecraft

A DragonForce ransomware attack typically follows a structured lifecycle from initial reconnaissance to final extortion. Below is a step-by-step overview of how a DragonForce attack might unfold:

1. **Reconnaissance:** DragonForce affiliates choose a target organisation based on opportunity or intent. This could involve scanning the internet for vulnerable systems (e.g., unpatched servers or exposed Remote Desktop Protocol (RDP)) or selecting a company known to have valuable data. If politically motivated, the target might be aligned with an ideological cause.
2. **Initial Intrusion:** The attackers gain entry to the network. For instance, an affiliate may send carefully crafted phishing emails to employees, luring one into downloading a malware loader. Alternatively, they exploit a known vulnerability on an internet-facing server (like an unpatched web application or VPN gateway) to get a foothold.
3. **Persistence:** After the initial compromise, the attackers work to entrench themselves. They might create new user accounts with high privileges or use tools to obtain password hashes from the compromised machine. They set up persistence mechanisms such as a backdoor service, or by scheduling tasks that will reinstate their access daily.
4. **Privilege Escalation:** With a foothold established, the attackers escalate their privileges to get domain administrator or equivalent control. They might exploit a local privilege escalation vulnerability or harvest an admin credential from the first machine.
5. **Lateral Movement and Network Discovery:** Using the admin credentials, the attackers access other servers and systems. They might use RDP to access a file server, or use the domain controller to push out tools to many machines. They scan for critical systems: file servers, database servers, email servers, backup servers. If certain high-value systems are on the network, they will make a note to target those for data theft and encryption. They also identify where backups are kept to plan how to destroy them.
6. **Data Collection and Exfiltration:** Before deploying ransomware, DragonForce operators prioritise stealing data quietly. They gather large collections of sensitive files. This can include financial records, databases, client data, email inboxes, and any confidential documents. These files are packaged (often into compressed archives) and then exfiltrated.
7. **Pre-Ransomware Attack Preparation:** With data in hand and network access everywhere, the attackers prepare for the ransomware detonation. They often disable security systems. Using their admin rights, they might uninstall or kill processes for anti-virus, endpoint detection and response (EDR), or other monitoring tools across the network. They also attempt to delete or encrypt backups.
8. **Ransomware Deployment and Encryption:** At the designated time, the ransomware binaries execute on infected machines throughout the network. Users might suddenly notice their files getting renamed or a slowdown as encryption proceeds.
9. **Victim Notification:** Then ransom notes start popping up. DragonForce's ransom note will contain instructions, often including an onion address to the negotiation site and a victim-specific ID or key.
10. **Negotiation Phase:** The victim is expected to contact the attackers via the provided channel (Tor chat site or messenger). When they do, the DragonForce affiliate (or operator) will engage in negotiation. They may provide a "proof of life" decryption of a few files to show their decryptor works, or screenshots of stolen data as evidence.
11. **Payment or Data Leak:** If the victim agrees to pay, the payment is made to a crypto wallet provided by the attackers. DragonForce then provides a decryption tool to restore files and promises to delete the stolen data from their servers.

12. **Post-Attack and Cleanup:** DragonForce and its affiliates will typically withdraw from the network after either being paid or releasing data.

Tradecraft

DragonForce and its affiliates employ a range of tactics, techniques, and procedures (TTPs) that combine both ransomware techniques and tactics reflecting the group's unique background and toolset. Below is an overview of their typical tradecraft:

Category	Tool / Malware Name	Purpose / Function	Notes
Remote Access	SystemBC, Cobalt Strike	Persistent access and command-and-control (C2)	SystemBC used as a backdoor proxy; Cobalt Strike used for beaconing and lateral movement
Credential Theft	Mimikatz, LaZagne	Harvesting credentials from memory and local apps	Used post-compromise to extract domain admin or local credentials from LSASS
Reconnaissance	Advanced IP Scanner, PingCastle	Network and Active Directory mapping	Used to identify file servers, domain controllers, and AD weaknesses
Privilege Escalation	BYOVD (e.g. Intel Driver Exploit)	Kernel-level escalation and AV/EDR bypass	Leverages vulnerable signed drivers to disable security products
Lateral Movement	PsExec, WMI, RDP	Move laterally across hosts in the network	Used to spread malware and access other systems with elevated credentials
Data Exfiltration	MEGA.nz, FTP/SFTP, HTTP servers	Stealing and uploading victim data before encryption	Exfiltrated archives often uploaded to MEGA or attacker-controlled infrastructure
Ransomware Deployment	Custom DragonForce Builder Payloads	File encryption and ransom note delivery	Payloads customised per victim via affiliate panel with timing and note variations
Defense Evasion	PowerShell, Script-based Tools	Execute malicious commands while avoiding detection	Living-off-the-land techniques to disable AV, clear logs, and blend in with admin tasks

Containment, Mitigations & Remediations

DragonForce ransomware campaigns likely involve exploiting both vulnerabilities (T1190[10]) and leaked credentials (T1078[11]) as an initial access vector. As such, it is strongly recommended that the following security measures are implemented to bolster defences against potential exploitation:

[10] Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®
[11] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®

- Maintain a strong, intelligence led patching policy that prioritises vulnerabilities that are under active exploitation or those that have a published proof of exploit
- Invest in dark web credential monitoring solutions to identify any leaked credentials before they can be used in an attempted attack. In 2024, 29% of ransomware attacks were likely initiated by the exploitation of compromised credentials[12].

Additionally, we strongly recommended that organisations implement the following defence strategies, in accordance with the Cybersecurity & Infrastructure Security Agency (CISA) standards, to mitigate against the threat of DragonForce ransomware compromise:

- Maintain offline, encrypted backups of critical data
- Implement a zero-trust architecture to prevent unauthorised access to data and services.

One primary method of reducing the threat of DragonForce ransomware is to detect it in the early stages through the utilisation of an effective and monitored EDR solution. A comprehensive EDR tool, such as the Microsoft Defender suite, can provide effective protection against malware threats, including DragonForce ransomware. These tools can block ransomware attempts once detected, alert system users to potential breaches, and halt the malware process during the early stages of the attack chain, thereby limiting the scope of damage.

Threat Assessment

Ransomware continues to be one of the prominent threats facing the private sector. Recent highly publicised attacks, combined with the evolving nature of ransomware infrastructure, have led to further high-profile attacks against large organisations in 2025 by groups incentivised by the potential for large ransom payouts.

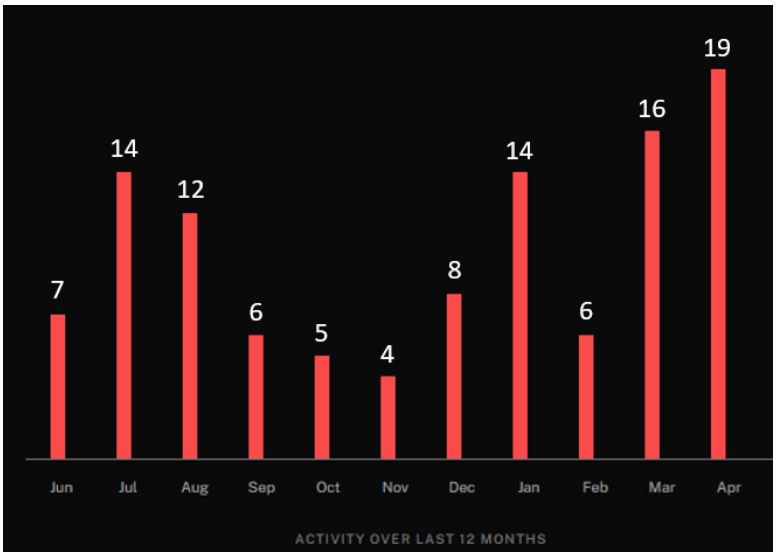


Figure 4: Global DragonForce ransomware frequency – 12 months.

Source: FalconFeeds

[12] 2024 Ransomware Report: Sophos State of Ransomware

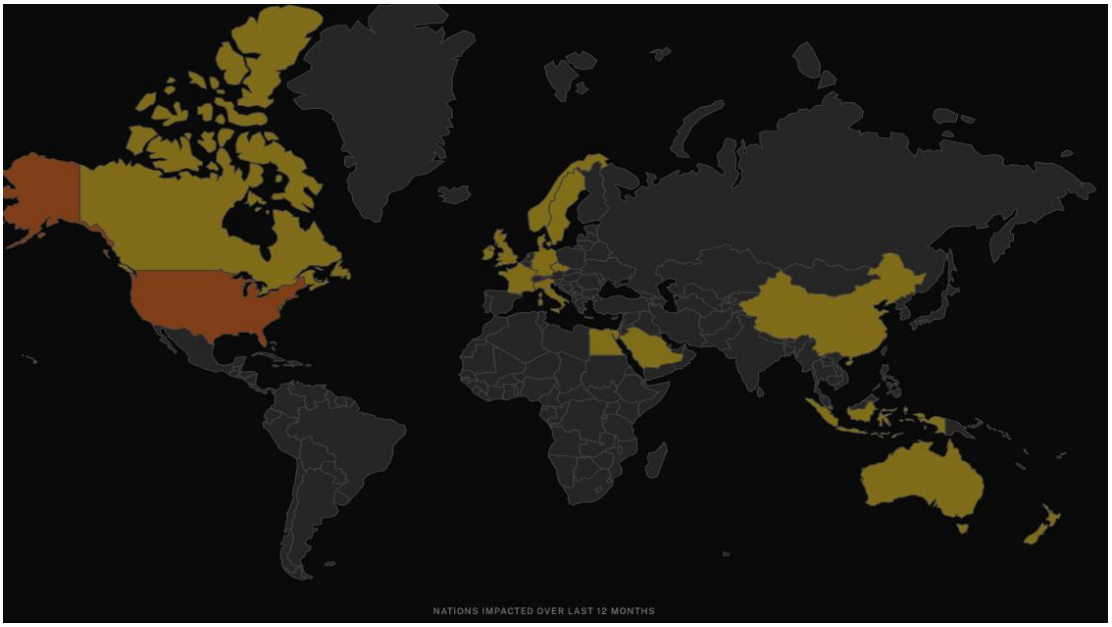


Figure 5: Global DragonForce targeting – 12 months.

Source: FalconFeeds

The likelihood of a DragonForce attack on any given organisation is currently **moderate to high**, especially as we move further into 2025. Its expansion through the RaaS model means it's built a growing network of affiliates actively hunting for vulnerable targets. This decentralised approach has broadened its reach and increased the pace of attacks.

The impact of a successful DragonForce attack can be **severe**. As shown in recent incidents, operations may be disrupted for days or even weeks, vast amounts of sensitive data may be encrypted or exfiltrated, and the recovery costs can be significant. Victims often face reputational damage, regulatory scrutiny, and, in many cases, large ransom demands.

DragonForce has shown above-average technical capability, both through its core team and affiliates. They make use of advanced tooling, adapt quickly to new vulnerabilities, and have demonstrated the ability to coordinate large-scale campaigns including simultaneous breaches across multiple organisations. Some affiliates, such as those linked to Scattered Spider, are skilled in social engineering and can bypass multi-factor authentication (MFA) using techniques like SIM swapping and phone impersonation.

Originally, DragonForce followed a cause-driven targeting pattern, often linked to its hacktivist roots, hitting organisations in countries like Israel or India. However, this has now shifted towards a more opportunistic model. Targets are selected based on exposure, perceived value, and likelihood of paying a ransom, regardless of geography or political stance.

Looking ahead, DragonForce is expected to continue **evolving and scaling**. Its introduction of white-label ransomware services and active affiliate recruitment through 2024 and into 2025 reflects a group that is maturing fast, not only in capability, but in its business model. It is clearly positioning itself as a flexible cybercrime platform rather than a single ransomware group.

In short, DragonForce should be seen as more than just another ransomware gang. It represents an ecosystem of adaptable threat actors, built around a professional infrastructure and capable of tailoring its attacks to different industries and regions. As it describes itself as a "ransomware cartel", its threat level is best assessed **as high and rising**.

Appendix A – Indicators of Compromise (IOC)

IOC Type	IOC Value	Comment
Ransom note	README.txt	Name of ransom note left in the directories of encrypted file
Ransom note	[rand].README.txt	Name of ransom note left in the directories of encrypted file
File extension	.df	File extension used by DragonForce
md5	9a218d69ecafe65eae264d2fdb52f1aa	File hashes used by DragonForce ransomware
md5	d44071f255785c73909d64f824331ebf	File hashes used by DragonForce ransomware
md5	b97812a2e6be54e725defbab88357fa2	File hashes used by DragonForce ransomware
md5	296cca79bbb3ca764de8fcdc2070ecc2	File hashes used by DragonForce ransomware
md5	d54bae930b038950c2947f5397c13f84	File hashes used by DragonForce ransomware
sha256	d626eb0565fac677fdc13fb0555967dc31e600c74fbbd110b744f8e3a59dd3f9	File hashes used by DragonForce ransomware
sha256	ba1be94550898eedb10eb73cb5383a2d1050e96ec4df8e0bf680d3e76a9e2429	File hashes used by DragonForce ransomware
sha256	822ceefb12b030f2ff28dcda6776addda77b041dbb48d2e3a8c305721f4cc8ef	File hashes used by DragonForce ransomware
sha256	1250ba6f25fd60077f698a2617c15f89d58c1867339bfd9ee8ab19ce9943304b	File hashes used by DragonForce ransomware
sha256	df903c620508011ca8eb2aaaf9712a526b31a12c800b856cd524ebb3fde854b2	File hashes used by DragonForce ransomware
sha256	55befb5de5d9bc45978efd1a960ae21ed81e4be9c6521aaeebf8d5884444e3c9	File hashes used by DragonForce ransomware

Sha1	196c08fbab4119d75afb209a05999ce269ffe3cf	File hashes used by DragonForce ransomware
Sha1	577b110a8bfa6526b21bb728e14bd6494dc67f71	File hashes used by DragonForce ransomware
Sha1	29baab2551064fa30fb18955ccc8f332bd68ddd4	File hashes used by DragonForce ransomware
Sha1	b571e60a6d2d9ab78da1c14327c0d26f34117daa	File hashes used by DragonForce ransomware
Sha1	e164bbaf848fa5d46fa42f62402a1c55330ef562	File hashes used by DragonForce ransomware
File	socks.exe	A backdoor associated with the SystemBC malware family DragonForce
File	a65.exe	A payload of Cobalt Strike DragonForce
File	netscanold.exe	A network scanning tool known as SoftPerfect Network Scanner DragonForce
File	df.exe	The ransomware file DragonForce
File path	C:\Users\username\AppData\Local\Temp\2\ socks aug\socks.exe	The file to the SystemBC malware DragonForce
File path	C:\Users\username\AppData\Local\Temp\ 2\a65.exe	The file path of the Cobalt Strike Beacon DragonForce
File path	df.exe (dropped in multiple paths)	Can found on multiple paths DragonForce
URL	z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion	DragonForce TOR Onion file servers of DragonForce
URL	z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion/blog	URL to DragonForce blog
URL	3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd[.]onion	TOR Onion file servers of DragonForce
URL	dragonforxxbp3awc7mzs5dkswrua3znqyx5roefmi4smjrsdi22xwqd[.]onion	TOR Onion file servers of DragonForce
URL	6dgi54prfmpuuolutr4hl3akasxbx4o34g5y2bj4blrvzzkjemhxenad[.]onion	TOR Onion file servers of DragonForce

URL	eogeko3sdn66gb7vjpwpmlmmmzfx7umtwaugpf5l6tb5jveolfydnuad[.]onion	TOR Onion file servers of DragonForce
URL	ewrxgpvv7wsrqq7itfwg5jr7lkc6zzknndmru5su2ugrowxo3wwy5yad[.]onion	TOR Onion file servers of DragonForce
URL	3ro23rujyigqrlrwk3e4keh3a3i6ntgrm3f42tbiqtf7vke47c6a6ayd[.]onion	TOR Onion file servers of DragonForce
URL	jziu7k7uee467r2wt66ndrwymmw7tsmqgcqi7aemcaxraqmaf2hdm3yd[.]onion	TOR Onion file servers of DragonForce
URL	2yczff6zyiey3gkgl5anwejktdp73abxbzbnvwobmrwkwgf3hudpyvyd[.]onion	TOR Onion file servers of DragonForce
URL	bpoowhokr3vi32l3t4mjdtdxfrfpigwachopk5ojwmgxihnojhsawuyd[.]onion	TOR Onion file servers of DragonForce
URL	dbvczza7nhwdb5kdvkzjtkrcvwnrt5viw7mihutueprvajy7rxhwq6id[.]onion	TOR Onion file servers of DragonForce
URL	xtcwd3xmxpggtizn7kmwwqeizexflkkyqsytg2kauccau6ddsfa4gfyd[.]onion	TOR Onion file servers of DragonForce
URL	4wcrfql53ljekid3sn66z6swjot725muveddq77utxltaelw64eikfid[.]onion	TOR Onion file servers of DragonForce
URL	73h3lxn24kuayyfkn4t6ij7e67jklo24vqzqdhpts3ygmim7hu6u6aid[.]onion	TOR Onion file servers of DragonForce
URL	nwtetzmrqhxieetg5lvth7szzvg35gfrqt23ly46vku56oo7pkueswyd[.]onion	TOR Onion file servers of DragonForce

Appendix B – MITRE ATT&CK

Tactic	Technique	ID	Analyst Comment
Reconnaissance	Valid Accounts	T1078[13]	DragonForce ransomware actors gain unauthorised access and blend in with legitimate user activity.
Initial Access	Phishing	T1566[14]	DragonForce ransomware actors send deceptive messages to trick users into disclosing sensitive information or executing harmful actions
Initial Access	External Remote Services	T1133[15]	The threat actor exploit vulnerabilities in external remote services, like VPNs, to gain unauthorised access to a network.
Execution	User Execution	T1204.002[16]	The DragonForce ransomware tricks users into opening malicious files to execute harmful code.
Execution	Command-Line Interface: PowerShell	T1059.001[17]	The threat actor users various command-line parameters for configuration and control
Persistence	Valid Accounts: Domain Accounts	T1078.002[18]	DragonForce ransomware gains unauthorised access and move laterally within networks.
Persistence	Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder	T1547.001[19]	Programs are added to startup folders or registry run keys to achieve persistence.
Persistence	Create or Modify System Process: Windows Service	T1543.003[20]	DragonForce ransomware creates or modifies Windows services to maintain persistence on compromised systems.
Defence Evasion	Impair Defences: Disable or Modify Tools	T1562.001[21]	DragonForce disables or modifies security tools to evade detection.
Defence Evasion	Scheduled Task/Job: Scheduled Task	T1053.005[22]	DragonForce exploit the Windows Task Scheduler to schedule tasks for executing malicious code.

[13] Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®
[14] Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®
[15] External Remote Services, Technique T1133 - Enterprise | MITRE ATT&CK®
[16] User Execution: Malicious File, Sub-technique T1204.002 - Enterprise | MITRE ATT&CK®
[17] Command and Scripting Interpreter: PowerShell, Sub-technique T1059.001 - Enterprise | MITRE ATT&CK®
[18] Valid Accounts: Domain Accounts, Sub-technique T1078.002 - Enterprise | MITRE ATT&CK®
[19] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®
[20] Create or Modify System Process: Windows Service, Sub-technique T1543.003 - Enterprise | MITRE ATT&CK®
[21] Impair Defenses: Disable or Modify Tools, Sub-technique T1562.001 - Enterprise | MITRE ATT&CK®
[22] Scheduled Task/Job: Scheduled Task, Sub-technique T1053.005 - Enterprise | MITRE ATT&CK®

Tactic	Technique	ID	Analyst Comment
Defence Evasion	Indicator Removal: Clear Windows Event Logs	T1070.001[23]	The threat actor clears Windows Event Logs to hide their activities
Credential Access	OS Credential Dumping: LSASS Memory	T1003.001[24]	The threat actor dumps LSASS memory to steal credential information
Discovery	File and Directory Discovery	T1083[25]	The threat actor enumerates logical drives and checks their types, discovering information about the computer's drives and directories
Discovery	Domain Trust Discovery	T1482[26]	The threat actor employs tools to gather information on Active Directory domain trusts
Discovery	Remote System Discovery	T1018[27]	The threat actor discovers remote systems on a network to facilitate lateral movement
Discovery	System Network Configuration Discovery	T1016[28]	The threat actor gathers information about network configurations and settings
Discovery	System Information Discovery	T1082[29]	The threat actor gathers detailed system information to understand the environment and plan further attacks
Discovery	Network Service Discovery	T1046[30]	The threat actor discovers services running on remote hosts and network devices, often using port and vulnerability scans
Lateral Movement	Remote Services: Remote Desktop Protocol	T1021.001[31]	The threat actor leverages Remote Desktop Protocol (RDP) to access and control remote systems
Lateral Movement	Remote Services: SMB/Windows Admin Shares	T1021.002[32]	The threat actor uses valid accounts to interact with remote network shares via SMB (Server Message Block) to move laterally within a network
Collection	Data from Local System	T1005[33]	While not explicitly mentioned, the ransomware collects information

[23] Indicator Removal: Clear Windows Event Logs, Sub-technique T1070.001 - Enterprise | MITRE ATT&CK®
[24] OS Credential Dumping: LSASS Memory, Sub-technique T1003.001 - Enterprise | MITRE ATT&CK®
[25] File and Directory Discovery, Technique T1083 - Enterprise | MITRE ATT&CK®
[26] Domain Trust Discovery, Technique T1482 - Enterprise | MITRE ATT&CK®
[27] Remote System Discovery, Technique T1018 - Enterprise | MITRE ATT&CK®
[28] System Network Configuration Discovery, Technique T1016 - Enterprise | MITRE ATT&CK®
[29] System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®
[30] Network Service Discovery, Technique T1046 - Enterprise | MITRE ATT&CK®
[31] Remote Services: Remote Desktop Protocol, Sub-technique T1021.001 - Enterprise | MITRE ATT&CK®
[32] Remote Services: SMB/Windows Admin Shares, Sub-technique T1021.002 - Enterprise | MITRE ATT&CK®
[33] Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®

Tactic	Technique	ID	Analyst Comment
			about files, directories, and drive types on the local system to decide what to encrypt
Command and Control	Application Layer Protocol: Web Protocols	T1071.001[34]	The threat actor communicates with command-and-control servers through web protocols to blend in with normal traffic
Exfiltration	Exfiltration Over C2 Channe	T1041[35]	While not explicitly mentioned, the ransomware may communicate with a command-and-control (C2) server as part of the extortion process
Impact	Data Encrypted for Impact	T1486[36]	The threat actor encrypts files using ChaCha8 encryption and the CryptGenRandom() function to generate keys and initialisation vectors (IVs) for each file
Impact	Inhibit System Recovery	T1490[37]	The threat actor deletes or disables system recovery features to prevent recovery of a corrupted system

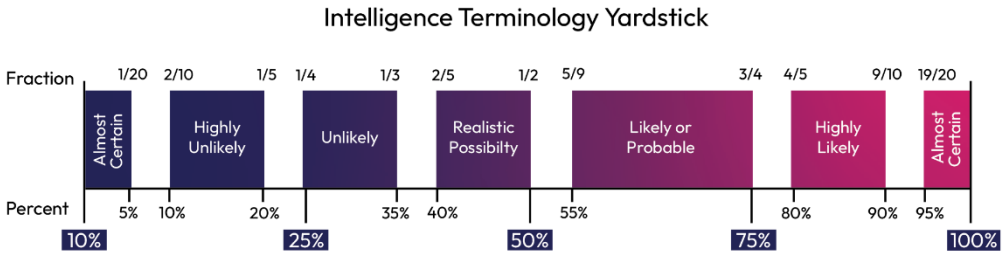
[34] Application Layer Protocol: Web Protocols, Sub-technique T1071.001 - Enterprise | MITRE ATT&CK®
[35] Exfiltration Over C2 Channel, Technique T1041 - Enterprise | MITRE ATT&CK®
[36] Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®
[37] Inhibit System Recovery, Technique T1490 - Enterprise | MITRE ATT&CK®

Appendix C – Terminology Yardstick

Intelligence Terminology Yardstick

Key assessments within this report have been written using the Intelligence Terminology Yardstick. The assessed likelihood of events corresponds with pre-defined language to remove areas of uncertainty when ingesting Quorum Cyber Threat Intelligence reports.

Intelligence Cut-off Date (ICoD): 12/05/2025 10:00 UTC



This threat report uses pre-defined language found within the Intelligence Terminlolgy Yardstick to express the likelihood of events.

Appendix D – Sources

- https://www.sentinelone.com/blog/dragonforce-ransomware-gang-from-hacktivists-to-high-street-extortionists
- https://www.group-ib.com/blog/dragonforce-ransomware/
- https://blog.checkpoint.com/security/dragonforce-ransomware-redefining-hybrid-extortion-in-2025
- https://medium.com/@tahirbalarabe2/the-rise-of-dragonforce-ransomware-ffc516836b32
- https://www.radware.com/security/ddos-knowledge-center/ddospedia/dragonforce-malaysia
- https://www.computerweekly.com/news/366623685/Chaos-spreads-at-Co-op-MS-following-DragonForce-attacks
- https://www.sentinelone.com/blog/dragonforce-ransomware-gang-from-hacktivists-to-high-street-extortionists
- https://securityaffairs.com/177376/cyber-crime/dragonforce-group-claims-the-theft-of-data-after-co-op-cyberattack.html
- https://www.sophos.com/en-us/content/state-of-ransomware
- https://thehackernews.com/2025/04/ransomhub-went-dark-april-1-affiliates.html