TLP:CLEAR

CENTRE FOR
CYBERSECURITY
BELGIUM

THREAT ACTOR PROFILE

DRAGONFORCE

CYBER THREAT INTELLIGENCE REPORT

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Date: 29 April 2026
Version: 1.0 EN
Author: Centre for Cybersecurity Belgium (CCB) - CyTRIS department

Intelligence cut-off date: 16 April 2026

Target audience:
Organisations seeking to strengthen their resilience against attacks by the DragonForce group and its affiliates.

Permitted distribution of TLP:CLEAR:
Information can be shared freely with anyone, without restrictions. More information: https://www.first.org/tlp/

Table of Contents

Executive summary **4**

Key Judgements *4*

Recommended Actions *5*

Scope *5*

Introduction **6**

Findings & Assessments **7**

Adversary *7*

Victimology *11*

Capabilities *15*

Infrastructure *18*

Conclusions **19**

Outlook *19*

Recommendations *19*

About the CCB **21**

References **23**

Appendices **26**

Appendix A: Indicators of Compromise (IOC Package) *26*

Appendix B: Ransom note *27*

Appendix C: Tactics, Techniques, and Procedures (TTP) *28*

Appendix D: Malware & Tools *30*

EXECUTIVE SUMMARY

DragonForce is a double extortion Ransomware-as-a-Service (RaaS) operator that emerged in December 2023 and has rapidly established itself as a significant and evolving cyber threat. The group demonstrates a dynamic and expansive character, marked by frequent changes in organisational structure and affiliations. To date, DragonForce has compromised over **400 victims**, including two Belgian organisations (one in construction and one in business services), which suffered operational downtime and the exposure of sensitive data.

Key Judgements

- It is assessed with medium confidence that DragonForce is exclusively financially motivated, with no indicators of political affiliation, ideological objectives, or nation-state sponsorship, based on consistent targeting patterns and the absence of ideological communication.
- It is assessed with medium confidence that the reported association with hacktivist group **DragonForce Malaysia is false flag in nature**, based on operational inconsistencies and attribution indicators suggesting CIS or Russian origin.
- It is assessed with high confidence that DragonForce primarily targets high-GDP Western nations, where the **United States constitutes the dominant target country**, based on victim data and observed incident distribution.
- Victim concentration is highest across **manufacturing, business services, technology, construction, and healthcare sectors**, based on aggregated victimology data. It is assessed with high confidence that this pattern reflects the deliberate targeting of economically valuable organisations with comparatively lower cybersecurity maturity.
- It is assessed with medium confidence that DragonForce **relies on European, predominantly UK-based ISPs** with partial use of **bulletproof hosting providers**, based on infrastructure analysis and observed network indicators.
- It is assessed with high confidence that operational tempo is on an expansion trajectory, driven by sustained financial incentives and the maturation of the group's RaaS affiliate model, based on affiliate recruitment activity and increasing victim volume.
- It is assessed with medium confidence that further consolidation within the ransomware ecosystem is likely, potentially through **absorption or co-option of rival groups**, based on observed patterns and historical precedent.

Recommended Actions

In addition to standard ransomware defences, the CCB strongly recommends implementing the following targeted protections[1]:

- **Phishing Attack Mitigations**: Regular security awareness training and phishing simulations; email security measures.
- **Remediation of Exploited Vulnerabilities**: Continuous patch management processes and vulnerability scans[2]; special attention to securing internet-facing systems and edge devices.
- **Protection Against Leaked or Stolen Credentials**: Multi-Factor Authentication; Privileged Access Management; dark web and OSINT monitoring to identify leaked or stolen credentials.
- **Utilisation of Threat Intelligence**: Leverage the IOC Package provided by the CCB tailored to detect DragonForce's activity, refer to Appendix A: Indicators of Compromise (IOC Package).

Scope

This report assesses the activities of **DragonForce** and its affiliated threat actors, focusing on their escalating operations, nuances in affiliations, changes in leadership, and the evolving nature of organised crime. It aims to help current and potential victims understand the threat and strengthen their defences against future attacks from this or similar groups.

The intelligence cut-off date is 16 April 2026.

[1] For more detailed guidance, refer to the subchapter titled „*Recommendations*".
[2] To prioritize the vulnerabilities, refer to the CCB's advisory page, available at: https://ccb.belgium.be/advisories.

INTRODUCTION

Ransomware attacks continue to rise, and this trend shows no signs of slowing down. One notable threat group, **DragonForce**, has seen a significant surge in activity following its emergence in December 2023. Their operations are causing considerable harm to victims, prompting closer analysis of their tactics and impact.

Background Context

Although ransom payments remain high, the median payment declined by approximately 50%, from $2 million in 2024 to $1 million in 2025, largely due to improved negotiation outcomes[3]. Despite this, nearly half of organisations still choose to pay the ransom to recover their data. Ransomware attacks frequently disrupt business continuity, with approximately 58% of affected organisations forced to halt operations during recovery[4]. Moreover, these incidents have significant business impacts: 40% of organisations report revenue losses, 41% lose customers, and 40% are forced to reduce their workforce[5]. At the same time, only 13% of organisations fully recover their data following a ransomware attack.

Ransomware attacks cause major disruptions, sometimes bringing systems to a complete halt, resulting in a pause in production until the issue is resolved. In addition, incident response can be extremely costly, requiring a specialized team and extensive recovery efforts, both time-consuming and expensive, adding further strain to the company. Once the immediate incident is over, the affected company may face customer backlash, legal fees, and potential lawsuits due to inadequate security measures that allowed the breach to occur. This leads to reputational damage, which can result in the loss of customers and a diminished market position.

These combined factors make **surviving a ransomware attack extremely difficult for companies**, even after they fully recover their systems and data. The average cost of an attack is estimated at **over $4.5 million**, not including long-term reputational damage[6].

[3] Sophos, *„Nearly Half of Companies Opt to Pay the Ransom, Sophos Report Finds”*, https://www.sophos.com/en-us/press/press-releases/2025/06/nearly-half-companies-opt-pay-ransom-sophos-report-finds, 24 May 2025.
[4] Infosecurity Magazine, “58% of Ransomware Victims Forced to Shut Down Operations”, https://www.infosecurity-magazine.com/news/ransomware-victims-shut-operations/, 19 March 2026.
[5] Help Net Security, *„Only 13% of organizations fully recover data after a ransomware attack”,* https://www.helpnetsecurity.com/2025/01/29/ransomware-attacks-business-operations-disruption/, 29 January 2025.
[6] Huntress, *„The Cost of Ransomware Attacks for Business”*, https://www.huntress.com/ransomware-guide/cost-of-ransomware-attacks, 25 May 2025.

FINDINGS & ASSESSMENTS

Adversary[7]

Motivation

DragonForce's primary motivation of the threat actor is **financial gain**, which is explained in multiple sections of the report later on. Choice of targets, methods, and few other aspects points towards this statement. No clear evidence was found linking the threat actor to nation-state-driven activities.

DragonForce employs a **double-extortion** strategy. Double extortion ransomware is a cyberattack where threat actors both steal sensitive information and encrypt data. This dual threat increases leverage, as failure to pay can result in stolen data being leaked, sold, or published - making the overall impact of the incident significantly more complex, costly, and difficult to manage than traditional ransomware alone.

Attribution[8]

False association with Malaysia and ties to CIS countries

There is a persistent misconception that DragonForce is a hacktivist group or originated as one called DragonForce Malaysia, often cited in multiple reports without substantiating evidence. In reality, **there is no valid evidence that DragonForce and DragonForce Malaysia are the same entities**. DragonForce Malaysia operates as a hacktivist actor, targeting governments and organisations perceived as hostile to Islamic nations or supportive of Israel. Conversely, DragonForce functions as a ransomware-as-a-service (RaaS) operator[9], with no current evidence supporting any hacktivist affiliation.

Supporting indicators of separation:

- DragonForce's operational rules prohibit attacks on Russia and other former Soviet Union states, but imposes no such restriction on Malaysia , suggesting a Commonwealth of Independent States (CIS)[10] or Russian origin[11].
- DragonForce Malaysia has publicly denied any involvement with RaaS operations[12].

[7] This section seeks to answer an investigative question: Who is responsible for threat actor's threat activity, and what are their likely motivations, affiliations, or strategic objectives?
[8] The CCB does not have the authority to attribute threat actors to their sponsors. Therefore, this intelligence is based on what other credible sources claim about attribution.
[9] SOCRadar, *„Dark Web Profile: DragonForce Ransomware"*, https://socradar.io/blog/dark-web-profile-dragonforce-ransomware/, 12 May 2025
[10] The Commonwealth of Independent States (CIS) is a group of former Soviet republics formed in 1991 after the dissolution of the Soviet Union to maintain cooperation. Its members have included: Russia, Ukraine, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan, Armenia, Azerbaijan, Georgia, and Moldova.
Britannica, "*Commonwealth of Independent States*", https://www.britannica.com/topic/Commonwealth-of-Independent-States, 19 March 2026.
[11] Barracuda, *„DragonForce Ransomware Cartel vs. Everybody"*, https://blog.barracuda.com/2025/06/09/dragonforce-ransomware-cartel-vs--everybody, 09 May 2025
[12] *Ibidem*.

Indicators supporting CIS or Russian origin attribution:

- Ransomware variants attributed to DragonForce are based on leaked builders linked to Russian cybercriminal groups[13].
- DragonForce markets its services on the Russian Anonymous Marketplace (RAMP), where communications primarily occur in Russian[14].
- In the context of escalating conflicts between DragonForce and RansomHub, a RansomHub spokesperson accused DragonForce of having contacts within the Russian FSB intelligence service. While this accusation suggests possible connections leveraged to undermine rival ransomware groups, there is no concrete evidence supporting the claim[15].

Affiliates Program

During its initial months, DragonForce established its 'DragonLeaks' dark web portal and conducted early attacks using payloads based on the leaked LockBit 3.0 builder, targeting organisations across multiple sectors and geographies, including entities in the United States, United Kingdom, Australia, Latin America, and Asia-Pacific. The group used this period to build credibility on underground forums before formalizing its operations.

The DragonForce affiliate program officially launched on June 26, 2024, offering affiliates 80% of ransom payments along with tools for attack management and automation[16]. Affiliates are provided access to a control panel allowing them to manage attacks in real time[17], alongside sections for client management, payload configuration, leak site publication, and revenue tracking.

DragonForce built its payload from two codebases derived from prior leaks. One variant is based on LockBit 3.0, allowing individuals coming from LockBit to adapt quickly. The other, initially claimed as original, was found upon analysis to be a variant of Conti V3, enhanced with new features such as the Bring Your Own Vulnerable Driver (BYOVD) technique[18]. In July 2024, DragonForce introduced a second Conti-based variant, allowing affiliates to customize and select configurations based on their operational needs[19].

In accordance with Anti-Money Laundering concerns, DragonForce uses multiple techniques to launder money from ransom payments. Funds, typically sent via BTC, are rapidly moved through numerous cryptocurrency wallets and decentralized platforms to obscure their origin and facilitate money laundering.

---

[13] *Ibidem*.
[14] *Ibidem*.
[15] LevelBlue, *"The Godfather of Ransomware? Inside DragonForce's Cartel Ambitions"*, https://www.levelblue.com/blogs/spiderlabs-blog/the-godfather-of-ransomware-inside-dragonforces-cartel-ambitions, 03 February 2026
[16] Group-IB, *„Inside the Dragon: DragonForce Ransomware Group"*, https://www.group-ib.com/blog/dragonforce-ransomware/, 25 September 2024.
[17] ARMS Cyber Defense, *„Threat Report: DragonForce Ransomware's Professional Approach to Chaos"*, https://www.armscyber.com/resources/blog/dragonforce-ransomware-a-professional-approach-to-chaos/, 1 October 2024.
[18] Group-IB, *„Inside the Dragon..."*.
[19] Cyber Security News, *„DragonForce Ransomware Attack Analysis - Targets, TTPs and IoCs"*, https://cybersecuritynews.com/dragonforce-ransomware-attack/, 21 August 2025.

Associations

LockBit and Ransomware Coalition

In mid-March 2024, the government of Palau was hit by a ransomware attack that locked up computers. Ransom notes from two hacking gangs were left behind, one from LockBit and one from DragonForce[20]. The Palau Ministry of Finance Chief Information Security Officer stated that no sensitive information had been exfiltrated, and while both LockBit and DragonForce had sent ransom notes, no further efforts were made to communicate with the Palau government[21].

The presence of both notes indicated that **DragonForce was using the leaked LockBit builder rather than maintaining an operational connection with LockBit**. The double ransom note can be interpreted as an error due to technical inadequacies.

Cartel Evolution

Over the course of 2025, DragonForce underwent a series of structural changes that significantly altered its operational model and its relationships with both affiliates and rival groups (Figure 1).

Figure 1: Evolution of DragonForce [22, 23, 24]

[20] Fortra, *„DragonForce Ransomware - What You Need To Know"*, https://www.tripwire.com/state-of-security/dragonforce-ransomware-what-you-need-know, 11 April 2024.
[21] SC Media, *"DragonForce ransomware claims denied by Palau"*, https://www.scworld.com/brief/dragonforce-ransomware-claims-denied-by-palau, 9 April 2024.
[22] CSO, *„LockBit, DragonForce, and Qilin form a 'cartel' to dictate ransomware market conditions"*, https://www.csoonline.com/article/4070290/lockbit-dragonforce-and-qilin-form-a-cartel-to-dictate-ransomware-market-conditions.html, 9 October 2025.
[23] Trend Micro, *"DragonForce"*, https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-dragonforce, 29 October 2025.
[24] GBHackers, *"Mapping the Emerging Alliance Between Qilin, DragonForce, and LockBit"*, https://gbhackers.com/emerging-alliance/, 19 December 2025.

DragonForce vs. BlackLock

After announcing its transition into a ransomware cartel, DragonForce aggressively moved against rival groups, launching harassment campaigns and defacing the leak site of competitor BlackLock within 24 hours[25]. DragonForce publicly defaced the BlackLock site and leaked configuration files, internal chats, and builder artifacts. Evidence suggests the action may have been coordinated, as BlackLock's codebase and DragonForce's appeared to be nearly identical, and BlackLock's admin showed no resistance, pointing to either a soft handover or strategic absorption under DragonForce's expanding umbrella rather than a purely hostile action[26].

DragonForce vs. RansomHub

DragonForce then turned its attention to RansomHub, whose infrastructure went offline on 01 April 2025. DragonForce claimed RansomHub had joined the cartel and created a dedicated portal for former RansomHub affiliates migrating to DragonForce branding. RansomHub pushed back publicly, with spokesperson accusing DragonForce of sabotage, internal betrayal, and cooperating with law enforcement[27]. Sophos researchers noted that the "collaboration" between DragonForce and RansomHub appeared to be more of a hostile takeover by DragonForce[28].

The nature of DragonForce's actions against both BlackLock and RansomHub remains analytically uncertain. The following hypotheses are assessed as plausible based on available evidence:

- **Hostile rivalry hypothesis**: eliminating a competitor or absorbing their affiliates can enlarge a group's market share, functioning as the cybercrime equivalent of a hostile takeover[29].
- **Concealment and rebrand hypothesis**: the victim group faked compromise to obscure its own presence and reemerge under a different identity or within the cartel structure, consistent with observed cases of RaaS groups rebranding after law enforcement pressure.
- **Voluntary consolidation hypothesis**: the "collaboration" may represent a voluntary merger, with former RansomHub affiliates migrating to DragonForce infrastructure - as has happened with the smaller group RansomBay, which is now also running on DragonForce systems[30].

No single hypothesis has been conclusively confirmed. Continued monitoring of affiliate migration patterns, payload overlap, and underground forum communications remains necessary to assess the true nature of these relationships.

[25] LevelBlue, „*The Godfather of Ransomware? Inside DragonForce's Cartel Ambitions*", https://www.levelblue.com/blogs/spiderlabs-blog/the-godfather-of-ransomware-inside-dragonforces-cartel-ambitions, 3 February 2026.
[26] Cybereason, "*Ransomware Gangs Collapse as Qilin Seizes Control*", https://www.cybereason.com/blog/threat-alert-qilin-seizes-control, 19 March 2026.
[27] LevelBlue, „*The Godfather of Ransomware?...*".
[28] Infosecurity Magazine, „*DragonForce Engages in "Turf War" for Ransomware Dominance*", https://www.infosecurity-magazine.com/news/dragonforce-turf-war-ransomware/, 23 May 2025.
[29] BlackFog, „*What Happens When Ransomware Gangs Attack Each Other?*", https://www.blackfog.com/when-ransomware-gangs-attack-each-other/, 24 July 2025.
[30] The Hacker News, „*RansomHub Went Dark April 1; Affiliates Fled to Qilin, DragonForce Claimed Control*", https://thehackernews.com/2025/04/ransomhub-went-dark-april-1-affiliates.html, 30 April 2025.

Scattered Spider

The threat actor **Scattered Spider** has been observed deploying DragonForce ransomware alongside its established intrusion techniques[31]. However, Scattered Spider is known to use multiple ransomware variants across operations. As such, the use of DragonForce likely reflects the adoption of an available ransomware service rather than evidence of a direct partnership or operational collaboration with the DragonForce group.

Activity

After emerging in 2023, the threat actor's activity has been increasing annually and is **projected to peak in 2026** based on current trends (Figure 2).

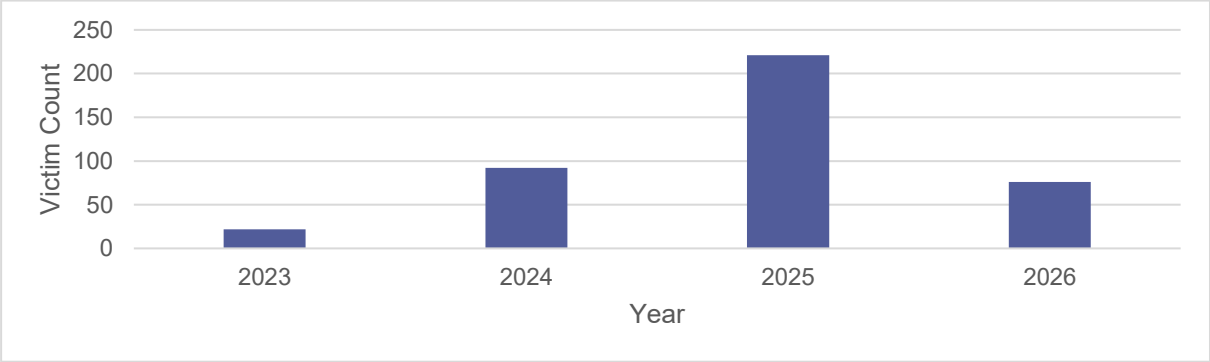

Figure 2: Activity of DragonForce over the years.

Victimology[32]

Regional Targeting

The threat actor primarily targets Western countries with high GDPs. The top 5 countries most targeted by this threat actor are: United States, Germany, Australia, France and Hong Kong (Figure 3). Among the victims, none were from The Commonwealth of Independent States.

Notably, the **United States** is the primary target country for this threat actor. The United States is an attractive target because it has the highest GDP in the world[33]. Additionally, the United States remains a significant hub for startups, SMEs (Small and Medium Enterprises), and a multitude of other companies. These organisations often lack sufficient resources to secure their networks but are valuable enough to be targeted for extortion.

[31] CISA, *„Joint Cybersecurity Advisory - Scattered Spider"*, https://www.ic3.gov/CSA/2025/250729.pdf, 29 July 2025.

[32] This section seeks to answer an investigative question: Who or what type of organisations or individuals are being targeted, and why are they specifically selected by threat actor?
Data is sourced from ransomware.live. A significant portion of fields, such as sector or country of victims, may be missing, so the graphs may not fully reflect reality.
Ransomware.live, *"Ransomware Statistics for Group: Dragonforce"*, https://www.ransomware.live/groupstats/dragonforce, 11 March 2026.

[33] World Bank Group, *"GDP (current US$)"*, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?view=map, 19 March 2026.

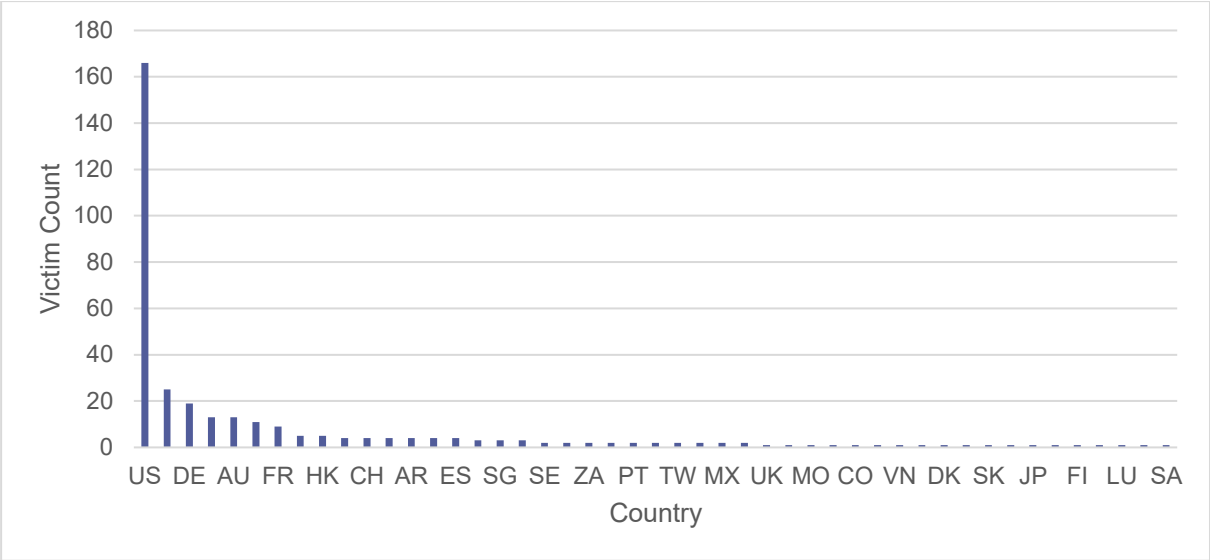

Figure 3: Countries targeted by DragonForce.

The targeting pattern also reflects a broader trend in which **SMEs are disproportionately affected**. These organisations often operate at a stage of growth where **resources are directed primarily toward business development, leaving cybersecurity investment at an early stage of maturity.**

Two organisations (one in construction and one in business services) have been recorded as victims of this ransomware threat actor[34]. Their compromise resulted in downtime and leakage of company's data.

Sectorial Targeting

The top five sectors most targeted by this threat actor are: Manufacturing, Business Services, Technology, Construction, and Healthcare.

Manufacturing is the most frequently targeted sector by the threat actor, followed closely by the **business services** and **technology** industries (Figure 4). All these sectors are known for their high economic value, which can be seen as a common factor. This target selection reinforces DragonForce's primary motivation - **monetary profit**. Organisations in **business services** and **manufacturing** are often lucrative yet relatively vulnerable targets. These industries tend to be **wealthy but not as well-defended** as sectors with stricter cybersecurity regulations. Their combination of high revenue and weaker security postures makes them attractive to ransomware operators.

[34] Ransomware.live, *„Belgian Victims of DragonForce"*, https://www.ransomware.live/id/UGVyc3luQGRyYWdvbmZvcmNl, 16 April 2026.

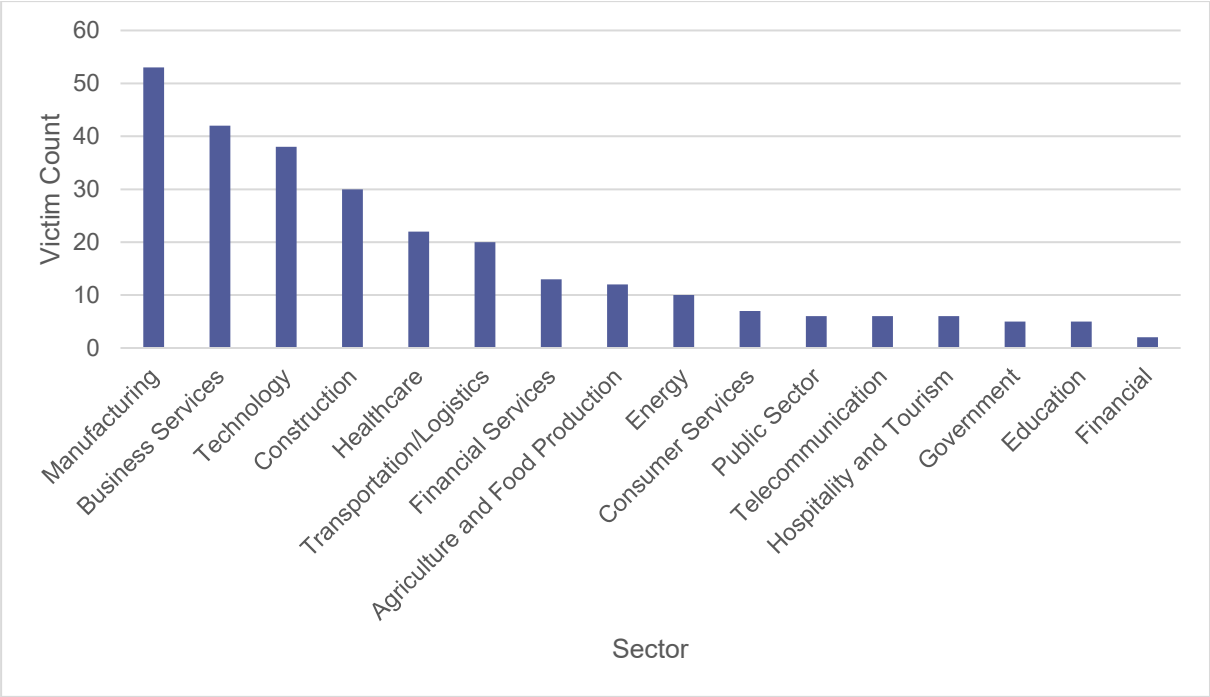

Figure 4: Sectors targeted by DragonForce.

Several interrelated factors likely make these sectors attractive to threat actors[35]:

- **Heavy reliance on technology**: These industries depend on digital infrastructure to maintain operational efficiency and competitiveness, significantly broadening their attack surface[36].
- **Outdated or vulnerable systems**: Many organisations within these sectors still operate legacy systems or lack modern security controls, increasing susceptibility to exploitation[37].
- **Limited cybersecurity resources**: Small and medium-sized enterprises (SMEs), including educational institutions and smaller manufacturers, often lack the financial and human resources necessary to implement robust cybersecurity programs[38], as cybersecurity tends to be a low priority, with investments directed to other areas of the business.
- **Complex and interconnected supply chains**: Industries such as automotive and manufacturing are deeply integrated into global supply networks. Disruption to these processes can create widespread impact, offering attackers increased leverage[39].

[35] Not all of the factors listed above apply equally to every sector mentioned. Some are strongly applicable to specific sectors, others less so — the intent is to highlight the broad characteristics that collectively make these industries attractive targets for threat actors.

[36] World Economic Forum, „*Global Cybersecurity Outlook 2025*”, https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf, 13 January 2025.

[37] Industrial Cyber, „*IBM X-Force reports evolving threat landscape amid shifting tactics, marking rise in stealth and identity exploits*”, https://industrialcyber.co/reports/ibm-x-force-reports-evolving-threat-landscape-amid-shifting-tactics-marking-rise-in-stealth-and-identity-exploits/, 21 April 2025.

[38] Cyber Readiness Insititute, “*Small and Medium-Sized Businesses Face Major Obstacles in Achieving Cyber Readiness: The State of SMB Cyber Readiness, 2024”,* https://cyberreadinessinstitute.org/news-and-events/small-and-medium-sized-businesses-face-major-obstacles-in-achieving-cyber-readiness-the-state-of-smb-cyber-readiness-2024/, 30 April 2024.

[39] Black Kite, „*2025 Manufacturing Report: Why Your Supply Chain is Your Biggest Cyber Risk*”, https://blackkite.com/report/manufacturing-tprm-report-2025/, 10 October 2025.

- **Critical data and operations**: These sectors frequently manage sensitive data or perform mission-critical functions. Threat actors target them knowing that any disruption could drive urgency in ransom negotiations[40].
- **Global exposure and regulatory risks**: Operating across borders exposes organisations to a wider range of threat actors and compliance challenges, complicating incident response and risk mitigation[41].
- **Fragility of operations:** Disruption of operations in these sectors often leads to costly repercussions and urgent remediation (such as paying the ransom)[42].

[40] Sophos, „*The State of Ransomware in Manufacturing and Production 2025*", https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-manufacturing-and-production-2025, 3 December 2025.
[41] World Economic Forum, „*Global Cybersecurity Outlook 2025*".
[42] Bitsight, „*Supply Chains Under Siege: Top 3 Cyber Threats to Manufacturing*", https://www.bitsight.com/blog/inside-cyber-threats-in-manufacturing-2025, 13 August 2025.

Capabilities[43]

Tools, Techniques, and Procedures (TTPs)

DragonForce's intrusion set does not feature novel techniques and largely overlaps with tradecraft common among other financially motivated threat actors. The following section maps DragonForce's observed techniques to the MITRE ATT&CK framework, organised by tactic stage.

Initial Access

DragonForce gains initial network access through multiple vectors, including phishing campaigns [T1566], exploitation of known software vulnerabilities [T1190] (e.g., Apache Log4j2, Ivanti Connect Secure), and brute-force attacks [T1110] targeting `RDP` and `VPN` services with common credentials such as "*administrator*," "*Admin*," "*rdpadmin*," and "*ftpadmin*."

Execution

Following initial access, the threat actor executes commands on compromised servers, often applying **Living Off the Land (LOTL)** approach[44, 45], using native system utilities such as `PowerShell` [T1059.001] to download and run malicious payloads, including `Cobalt Strike` beacons. The group also deploys cracked software and keygens across multiple endpoints [T1204] to further compromise the environment.
The dragonforce.exe ransomware can be executed through several methods, including `Windows Command Shell` [T1059.003] commands or exploiting shared modules and DLL hijacking [T1574.001] techniques.

Persistence

To maintain long-term access, the group uses compromised admin accounts [T1078] and disables security services by modifying registry keys [T1112], undermining system protections. Power settings are also altered to prevent shutdowns or reboots [T1490], further reinforcing malware persistence. The Threat actor also used `Schtasks.exe` [T1053.005] and `Taskkill.exe` [T1489] to establish persistence.

Privilege Escalation

The threat actor escalates privileges by dumping credentials from registry hives [T1003.002] to access sensitive operating system accounts. DragonForce ransomware has used access token manipulation [T1134], specifically token impersonation. This lets it run processes as `NT AUTHORITY\SYSTEM`, enabling high-impact actions across the environment.

Defence Evasion

DragonForce deploys **EDR-killing tools**[46] via **Bring Your Own Vulnerable Driver** techniques [T1068],

[43] This section seeks to answer an investigative question: What specific methods, tools, techniques, and tactics does threat actor use to achieve their objectives?
All tools utilised by the threat actor are listed in *"Appendix D: Malware & Tools"*.
All techniques employed by threat actor are covered in "*Appendix C: Tactics, Techniques, and Procedures (TTP)*".
[44] These techniques are described in chapter: „Tools, Techniques, and Procedures (TTPs)".
[45] These tools, while not inherently malicious, are repurposed to conduct malicious activities on compromised systems. The threat actor also makes use of **penetration testing frameworks**, software utilities, and native functions and services commonly used in legitimate environments, but which can be exploited to support malicious operations.
[46] ESET, "*EDR killers explained: Beyond the drivers*", https://www.welivesecurity.com/en/eset-research/edr-killers-explained-beyond-the-drivers/, 16 March 2026.

exploiting vulnerabilities in drivers such as `truesight.sys` and `rentdrv2.sys` to terminate security processes and bypass endpoint protections. Additionally, the ransomware deletes files [T1070.004], alters timestamps [T1070.006], and manipulates security tools [T1562.001] to evade detection and hinder remediation.

Credential Access

After compromising a system, DragonForce uses tools like `PassView`, `Mimikatz`, and `LaZagne` to harvest credentials [T1003] and map the environment. This helps it move laterally and escalate privileges across the network.

Discovery

DragonForce conducts discovery to map and understand victim environments, including identifying remote systems, application windows, network connections, and configurations. The ransomware can also detect sandboxed or debugging environments [T1497] to prevent execution in monitored settings. Key techniques include:

- Network [T1016] and account discovery [T1087] using tools such as `AdFind`.
- Exploitation of vulnerabilities in `SimpleHelp RMM`
- to gather device names, system configurations, user account details, and network connection data [T1082].

Lateral Movement

DragonForce moves laterally using native Windows tools, remote execution methods, and exploited third-party software. `RDP` [T1021.001] and `SMB` [T1021.002] are commonly leveraged to access additional systems. Vulnerabilities in `SimpleHelp RMM` are exploited to expand access and gather environment information. Key techniques include:

- `PsExec` - executing commands on remote systems [T1569.002]
- `Windows Management Instrumentation (WMI)` - remote command execution and system management [T1047].

Collection

The threat actor transfers and uses malicious tools and scripts to compromise systems and collect sensitive information. Data is identified, gathered, and staged for exfiltration [T1074] using a combination of built-in administrative utilities and third-party tools, often in preparation for ransomware deployment.

Command and Control

DragonForce maintains command and control (C2) through multiple channels to communicate with compromised systems. The group uses ingress tool transfer techniques, commonly via `FTP`, [T1105] to move tools from adversary-controlled infrastructure into victim networks. Additional delivery methods include `certutil.exe` [T1105] and `PowerShell` [T1059.001], as well as C2 over standard web protocols [T1071.001] to blend in with legitimate traffic.

Remote access tools, including `Cobalt Strike` and `SystemBC` [T1219], are also employed to facilitate command execution and maintain persistent access.

Exfiltration

Data exfiltration is central to DragonForce's double extortion strategy. Sensitive information is

collected and transmitted from the victim environment prior to encryption, enabling the threat actor to threaten public disclosure if ransom demands are not met.

Exfiltration channels include `SFTP`, `WebDAV`, `HTTP/S`, `FTP` servers, cloud storage platforms such as `MEGA`, and DragonForce's dedicated leak site (DLS) [T1041].

Impact

DragonForce ransomware [T1486] targets a wide range of enterprise environments, including **Windows** systems, **Linux** servers, **virtualized infrastructure** such as VMware ESXi, and **network-attached storage** devices. This cross-platform capability enables disruption of both endpoint systems and shared infrastructure.

The ransomware employs modern encryption techniques, using symmetric encryption for file contents and asymmetric cryptography to protect the keys. This ensures that victims cannot recover their data without the corresponding decryption material.

Ransom Note[47]

DragonForce left several noteworthy hints in one of their ransom notes post-infection that are worth examining. The threat actor specifically cuts ties with any political affiliation and emphasizes a strictly **financial motivation** with the statement: *"We work for money and are not associated with politics."* Moreover, they reassure the victim that the ransomware is reversible by stating: *"We decrypt 1 file to confirm that our decryptor works,"* confirming the **effectiveness of their ransomware**. This is important as many ransomware operators have faulty decryption mechanism or fail to decrypt files after receiving payment. Such approach encourages the victim to pay the ransom by displaying some level of assurance. The last part summarizes the note with a **standard extortion tactic**: pay, or we will release your data.

Vulnerabilities

The identified technologies targeted by the threat actor primarily consist of **internet-facing access and security appliances**, including VPN gateways, remote access tools, firewalls, and proxy systems (Table 1). These assets are typically deployed at the **network perimeter**, where they facilitate authentication, enforce access control policies, and enable remote connectivity to internal resources.
Due to their role as **gatekeepers between external and internal environments**, these systems represent **high-value targets for threat actors**. Successful exploitation can provide attackers with **initial access**, allowing them to bypass traditional perimeter defences and establish a foothold within the network. The most common targets were products of **Ivanti and Fortinet**.

[47] Full ransom note can be found in *"Appendix B: Ransom note"*.

CVE	CVSS	Name of Product	Type of Product
CVE-2024-57727	9.1	SimpleHelp remote support software	Remote access tool
CVE-2024-57728	9.1	SimpleHelp remote support software	Remote access tool
CVE-2024-57726	9.9	SimpleHelp remote support software	Remote access tool
CVE-2023-46805	8.2	Ivanti Connect Secure; Ivanti Policy Secure	VPN
CVE-2024-40766	9.3	SonicWall SonicOS	Firewall
CVE-2024-55591	9.8	Fortinet FortiOS; FortiProxy	Firewall / Proxy
CVE-2024-21412	8.1	Microsoft Windows Internet Shortcut Files	File format
CVE-2021-44228	10	Apache Log4j2	Software library
CVE-2024-21887	9.1	Ivanti Connect Secure; Ivanti Policy Secure	VPN
CVE-2024-21893	8.2	Ivanti Connect Secure; Ivanti Policy Secure	VPN
CVE-2024-21762	9.8	Fortinet FortiOS; FortiProxy	Firewall / Network

Table 1: Vulnerabilities exploited by the threat actor.

Infrastructure[48]

From the identified IP addresses, the threat actor predominantly leveraged European infrastructure, particularly UK-based ISPs. Many of these addresses originate from bulletproof hosting providers, shell companies, or networks with documented ties to criminal activity, including entities subject to international sanctions, as well as those repeatedly associated with phishing campaigns and the distribution of various malware families. Notable examples include:

- Global Connectivity Solutions LLP[49, 50].
- QWINS LTD[51]
- Alviva Holding Limited[52]
- Datacamp Limited[53, 54].

The threat actor maintains anonymity by using proxies, VPNs, and bulletproof hosting networks - environments where activities are largely uncontrolled and obscured from analysis and authorities.

[48] This section seeks to answer an investigative question: What infrastructure (e.g., C2 servers, hosting providers, domains, IP addresses) is used by the threat actor to conduct or support their operations?
[49] GBHackers, *„Russian Hackers Leverage Bulletproof Hosting to Shift Network Infrastructure”,* https://gbhackers.com/russian-hackers-leverage-bulletproof-hosting/, 31 March 2025.
[50] Qurium, *“How Russia uses EU companies for propaganda”*, https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/, 11 July 2024.
[51] IntelInsights, *“Bulletproof Hosting Hunt”,* https://intelinsights.substack.com/p/bulletproof-hosting-hunt, 27 July 2025
[52] The Raven File, *“Uncovering ALVIVA HOLDING: Links to Russian Shell Companies and Cybercrime”*, https://theravenfile.com/2025/09/08/uncovering-alviva-holding-links-to-russian-shell-companies-and-cybercrime/, 8 September 2025.
[53] Border Cyber Group, *„Rethinking trust in an age of proxy surveillance”,* https://bordercybergroup.com/rethinking-trust-in-an-age-of-proxy-surveillance/, 1 August 2025.
[54] GlobeNewswire, “IBCAP-Coordinated Lawsuit Results in $3 Million Settlement from U.K.-Based Content Delivery Network and Server Host, Datacamp Limited”, https://www.globenewswire.com/news-release/2024/02/05/2823594/0/en/IBCAP-Coordinated-Lawsuit-Results-in-3-Million-Settlement-from-U-K-Based-Content-Delivery-Network-and-Server-Host-Datacamp-Limited.html, 5 February 2024.

CONCLUSIONS

Outlook

The Centre for Cybersecurity Belgium assesses with **high confidence** that DragonForce's operations will continue to expand, driven by its financial motivations and evolving RaaS model. This assessment is based on observed annual increases in activity, its strategic alliances with affiliates, implications of changes in RaaS underground, and its evolution of ransomware build.

With **medium confidence**, CCB assesses that DragonForce will seek further consolidation within the ransomware ecosystem, potentially absorbing more rival groups to enhance its operational reach and capabilities.

Recommendations

Specific Recommendations

To protect an organisation from the DragonForce group, it is essential to address the primary intrusion methods they employ (Figure 7). The following measures should be implemented. Each countermeasure is linked to the cybersecurity framework **CyberFundamentals ESSENTIAL**, which provides guidance on proper implementation methods.

Vector of Attack	Remediations
Phishing Attacks: DragonForce frequently uses phishing to gain initial access.	• Employee Awareness Training - Regular security awareness programs to help employees recognize and report phishing attempts (PR.AT-1). • Email Security Measures - Deploy robust email filtering solutions to block malicious attachments and links (PR.PS-05). • Red Team Social Engineering Exercises - Conduct simulated phishing campaigns to assess and improve employee resilience (PR.AT-01.4).
Exploiting Vulnerabilities: DragonForce exploits high-severity vulnerabilities in edge devices.	• Continuous Patch Management - Regularly update operating systems, applications, and firmware to address known vulnerabilities (ID.AM-08). • Vulnerability Scanning & Remediation - Perform routine vulnerability assessments and remediate critical issues promptly (ID.RA-01).
Use of Leaked or Stolen Credentials: DragonForce leverages compromised credentials available on criminal forums or the dark web.	• Dark Web & OSINT Monitoring - Actively monitor for leaked credentials, compromised assets (RDP, VPN, web shells), and unauthorised access being sold. • Multi-Factor Authentication (MFA) - Enforce MFA across critical systems to minimize the impact of credential theft (PR.AA-03.2). • Privileged Access Management (PAM) - Limit and monitor the use of administrative accounts to reduce the attack surface (PR.AA-05.9)

Figure 7: Vectors of attack and specific countermeasures.

IOC Package

To address the threat of DragonForce, it is highly recommended to use the IOC package provided by the CCB. This package provides valuable threat indicators, detection rules, and mitigation strategies. For more information, refer to Appendix A: Indicators of Compromise (IOC Package).

Generic Recommendations

Additionally, CyTRIS highly recommends all entities to implement the CyberFundamentals framework.

Any organisation should start with the top 6 fundamental security controls:

- Protect remote access with **multifactor authentication**.
- Install the latest **security patches** regularly, with a priority for internet facing infrastructure.
- Install an **antivirus solution** on all endpoints.
- Secure your network with a **firewall** and **Wi-Fi encryption**.
- **Backup** all data regularly, including an offline backup disconnected from the network.
- Use **dedicated privileged accounts** for administrative tasks (and regular accounts for daily tasks.)

Full guidance on these 6 fundamental controls can be found in the CyFun® SMALL document.

As soon as these security controls are implemented, start to increase the organisations cybersecurity posture by implementing the (core) security controls of:

1. CyFun® BASIC, countering **82%** of the known attacks.
2. CyFun® IMPORTANT, countering **94%** of the known attacks.
3. CyFun® ESSENTIAL, countering **100%** of the known attacks.

These recommendations cannot replace a security roadmap. We strongly encourage all entities to conduct their own risk assessment to create a tailored security plan.

ABOUT THE CCB

The **Centre for Cybersecurity Belgium (CCB)** is the national authority for cybersecurity in Belgium. The CCB supervises, coordinates and monitors the application of the Belgian cyber security strategy. Through optimal information exchange, companies, the government, providers of essential services and the population can protect themselves appropriately.

The Centre for Cybersecurity Belgium (CCB) was established by Royal Decree of 10 October 2014 and operates under the authority of the Prime Minister.

The **CyTRIS (Cyber Threat Research and Intelligence Sharing)** Department of the Centre for Cybersecurity Belgium monitors cyber threats and publishes regular reports. The team collects, analyses and distributes information on threats, vulnerabilities and attacks on the information and communication systems of Belgium's vital sectors (critical infrastructure, government systems, critical data).

CyTRIS is also responsible for the Early Warning System (EWS). The EWS includes the information exchange platforms of the Belgian CSIRT. CyTRIS is responsible for the operational communication and information exchange with other national CSIRTs. CyTRIS also provides the “Spear Warning” procedure. A “Spear Warning” is an individual warning about an infection or vulnerability sent to organisations.

The CCB Connect & Share events, such as the Quarterly Cyber Threat Report (QCTR) events organised by CyTRIS, bring together different stakeholders and consultation platforms at least once a quarter and inform all participants as well as the Organisations of Vital Interest about the active cyber threats. At the QCTR event, the operation of the Early Warning System (EWS) is also discussed. Through this platform, the CyTRIS Team sends pertinent and analysed threat information to national security agencies, Vital Interest Organisations, their sectoral authorities and other partners.

Our events are also offered as a webinar and are open to anyone, for prior editions check out our YouTube channel: https://www.youtube.com/@cybersecuritybelgium.

DISCLAIMER

This document and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister.

This document contains technical information written mainly in English. Indeed, this technical information is taken directly from reports communicated to the CCB by various international partners (European network of CSIRTs, international organisations, foreign companies, etc.), which are written in English. Moreover, this information related to the security of networks and information systems is addressed to the organisations concerned under the benefit of urgency and to IT services which use the English terms of computer language.

A translation into Dutch, French or German of this technical information can nevertheless be requested from the CCB.

The CCB accepts no responsibility for the content of this document.

The information provided:

- is of a general nature and does not intend to take into consideration all particular situations;
- is not necessarily exhaustive, precise or up-to-date on all points;

Responsible editor:
Centre for Cybersecurity Belgium
Mr. M. De Bruycker, General Director
Rue de la Loi, 18
1000 Brussels

REFERENCES

1. Acronis, "*The DragonForce Cartel: Scattered Spider at the gate*", https://www.acronis.com/en/tru/posts/the-dragonforce-cartel-scattered-spider-at-the-gate/, 4 November 2025.
2. AML Network, "*DragonForce Ransomware*", https://amlnetwork.org/watchdog-database/cryptocurrency-laundering/dragonforce-ransomware/, 18 March 2026.
3. ARMS Cyber Defense, „*Threat Report: DragonForce Ransomware's Professional Approach to Chaos*", https://www.armscyber.com/resources/blog/dragonforce-ransomware-a-professional-approach-to-chaos/, 1 October 2024.
4. Barracuda, „*DragonForce Ransomware Cartel vs. Everybody*", https://blog.barracuda.com/2025/06/09/dragonforce-ransomware-cartel-vs--everybody, 09 May 2025
5. Bitdefender, "*DragonForce: The Ransomware Cartel Guarding Its Burrow*", https://businessinsights.bitdefender.com/dragonforce-ransomware-cartel, 4 June 2025.
6. Bitsight, „*Supply Chains Under Siege: Top 3 Cyber Threats to Manufacturing*", https://www.bitsight.com/blog/inside-cyber-threats-in-manufacturing-2025, 13 August 2025.
7. Black Kite, „*2025 Manufacturing Report: Why Your Supply Chain is Your Biggest Cyber Risk*", https://blackkite.com/report/manufacturing-tprm-report-2025/, 10 October 2025.
8. BlackFog, „*What Happens When Ransomware Gangs Attack Each Other*?", https://www.blackfog.com/when-ransomware-gangs-attack-each-other/, 24 July 2025.
9. Border Cyber Group, „*Rethinking trust in an age of proxy surveillance*", https://bordercybergroup.com/rethinking-trust-in-an-age-of-proxy-surveillance/, 1 August 2025.
10. Britannica, "*Commonwealth of Independent States*", https://www.britannica.com/topic/Commonwealth-of-Independent-States, 19 March 2026.
11. Broadcom, "*DragonForce Ransomware's Campaign Intensifies in 2025*", https://www.broadcom.com/support/security-center/protection-bulletin/dragonforce-ransomware-s-campaign-intensifies-in-2025, 16 April 2025.
12. CISA, "*CISA and Partners Release Updated Advisory on Scattered Spider Group*", https://www.cisa.gov/news-events/alerts/2025/07/29/cisa-and-partners-release-updated-advisory-scattered-spider-group, 29 July 2025.
13. CISA, „*Joint Cybersecurity Advisory - Scattered Spider*", https://www.ic3.gov/CSA/2025/250729.pdf, 29 July 2025.
14. CISA, "*Scattered Spider*", https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a, 29 July 2025.
15. CSO, „*LockBit, DragonForce, and Qilin form a 'cartel' to dictate ransomware market conditions*", https://www.csoonline.com/article/4070290/lockbit-dragonforce-and-qilin-form-a-cartel-to-dictate-ransomware-market-conditions.html, 9 October 2025.
16. CybelAngel, "*LockBit, Qilin, and DragonForce: The New Ransomware Alliance*", https://cybelangel.com/blog/lockbit-qilin-and-dragonforce/, 5 November 2025.
17. Cyber Press, "*DragonForce Ransomware Campaign Steals Sensitive Information From Businesses*", https://cyberpress.org/dragonforce-ransomware-steals-data/, 5 February 2026.
18. Cyber Readiness Institute, "*Small and Medium-Sized Businesses Face Major Obstacles in Achieving Cyber Readiness: The State of SMB Cyber Readiness, 2024*", https://cyberreadinessinstitute.org/news-and-events/small-and-medium-sized-businesses-face-major-obstacles-in-achieving-cyber-readiness-the-state-of-smb-cyber-readiness-2024/, 30 April 2024.
19. Cyber Security News, „*DragonForce Ransomware Attack Analysis - Targets, TTPs and IoCs*", https://cybersecuritynews.com/dragonforce-ransomware-attack/, 21 August 2025.
20. Cyber Security News, "*Researchers Breakdown DragonForce Ransomware Along with Decryptor for ESXi and Windows Systems*", https://cybersecuritynews.com/researchers-breakdown-dragonforce-ransomware/, 14 January 2026.
21. Cybereason, "*Ransomware Gangs Collapse as Qilin Seizes Control*", https://www.cybereason.com/blog/threat-alert-qilin-seizes-control, 19 March 2026.
22. Cybernews, "*Report: LockBit, Qilin, DragonForce join forces as ransomware cartel*", https://cybernews.com/security/lockbit-qilin-dragonforce-ransomware-cartel/, 10 October 2025.
23. Cybersecurity News, "*Ransomware Clash: DragonForce vs. RansomHub. No Honor Among Thieves*", https://cybersecurityventures.com/ransomware-clash-dragonforce-vs-ransomhub-no-honor-among-thieves/, 11 July 2025.
24. Cyble, "*Threat Actor Profile: DragonForce Ransomware Group*", https://cyble.com/threat-actor-profiles/dragonforce-ransomware-group/, 20 February 2025.
25. Darktrace, "*Tracking a Dragon: Investigating a DragonForce-affiliated ransomware attack with Darktrace*", https://www.darktrace.com/blog/tracking-a-dragon-investigating-a-dragonforce-affiliated-ransomware-attack-with-

darktrace, 5 November 2025.
26. FortiGuard Labs, "*DragonForce Ransomware*", https://www.fortiguard.com/threat-actor/6251/dragonforce-ransomware, 19 March 2026.
27. Fortra, „*DragonForce Ransomware - What You Need To Know*", https://www.tripwire.com/state-of-security/dragonforce-ransomware-what-you-need-know, 11 April 2024.
28. GBHackers, "*DragonForce Ransomware Targets Critical Businesses to Exfiltrate Sensitive Data*", https://gbhackers.com/dragonforce-ransomware-2/, 5 February 2026.
29. GBHackers, "*Mapping the Emerging Alliance Between Qilin, DragonForce, and LockBit*", https://gbhackers.com/emerging-alliance/, 19 December 2025.
30. GBHackers, „*Russian Hackers Leverage Bulletproof Hosting to Shift Network Infrastructure*", https://gbhackers.com/russian-hackers-leverage-bulletproof-hosting/, 31 March 2025.
31. GlobeNewswire, "IBCAP-Coordinated Lawsuit Results in $3 Million Settlement from U.K.-Based Content Delivery Network and Server Host, Datacamp Limited", https://www.globenewswire.com/news-release/2024/02/05/2823594/0/en/IBCAP-Coordinated-Lawsuit-Results-in-3-Million-Settlement-from-U-K-Based-Content-Delivery-Network-and-Server-Host-Datacamp-Limited.html, 5 February 2024.
32. Group-IB, "*DragonForce*", https://www.group-ib.com/masked-actors/dragonforce/, 18 March 2026.
33. Group-IB, „*Inside the Dragon: DragonForce Ransomware Group*", https://www.group-ib.com/blog/dragonforce-ransomware/, 25 September 2024.
34. Help Net Security, „*Only 13% of organizations fully recover data after a ransomware attack*", https://www.helpnetsecurity.com/2025/01/29/ransomware-attacks-business-operations-disruption/, 29 January 2025.
35. HelpNetSecurity, "*EDR killers are now standard equipment in ransomware attacks*", https://www.helpnetsecurity.com/2026/03/19/edr-killer-ransomware-attacks/, 19 March 2026.
36. Huntress, „*The Cost of Ransomware Attacks for Business*", https://www.huntress.com/ransomware-guide/cost-of-ransomware-attacks, 25 May 2025.
37. IC3, "*Scattered Spider*", https://www.ic3.gov/CSA/2025/250729.pdf, 29 July 2025.
38. Industrial Cyber, "*DragonForce reemerges as Conti-linked ransomware cartel, aligning with Scattered Spider in global attacks*", https://industrialcyber.co/ransomware/dragonforce-reemerges-as-conti-linked-ransomware-cartel-aligning-with-scattered-spider-in-global-attacks/, 6 November 2025.
39. Industrial Cyber, „*IBM X-Force reports evolving threat landscape amid shifting tactics, marking rise in stealth and identity exploits*", https://industrialcyber.co/reports/ibm-x-force-reports-evolving-threat-landscape-amid-shifting-tactics-marking-rise-in-stealth-and-identity-exploits/, 21 April 2025.
40. Infosecurity Magazine, "58% of Ransomware Victims Forced to Shut Down Operations", https://www.infosecurity-magazine.com/news/ransomware-victims-shut-operations/
41. Infosecurity Magazine, „*DragonForce Engages in "Turf War" for Ransomware Dominance*", https://www.infosecurity-magazine.com/news/dragonforce-turf-war-ransomware/, 23 May 2025.
42. IntelInsights, "*Bulletproof Hosting Hunt*", https://intelinsights.substack.com/p/bulletproof-hosting-hunt, 27 July 2025
43. LevelBlue, „*The Godfather of Ransomware? Inside DragonForce's Cartel Ambitions*", https://www.levelblue.com/blogs/spiderlabs-blog/the-godfather-of-ransomware-inside-dragonforces-cartel-ambitions, 3 February 2026.
44. Loginsoft, "*DragonForce Ransomware: Technical Analysis and Mitigation Strategies*", https://www.loginsoft.com/post/dragonforce-ransomware-technical-analysis-and-mitigation-strategies, 23 September 2025.
45. Malpedia, "*DragonForce*", https://malpedia.caad.fkie.fraunhofer.de/details/win.dragonforce, 18 March 2026.
46. Medium, "*Detailed Analysis of DragonForce Ransomware*", https://medium.com/s2wblog/detailed-analysis-of-dragonforce-ransomware-25d1a91a4509, 14 January 2026.
47. MITRE ATT&CK, "*Enterprise Matrix*", https://attack.mitre.org/matrices/enterprise/, 18 March 2026.
48. Proven Data, "*DragonForce Ransomware: Response, Recovery, Prevention, Background*", https://www.provendata.com/blog/dragonforce-ransomware/, 8 January 2026.
49. Qurium, "*How Russia uses EU companies for propaganda*", https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/, 11 July 2024.
50. Ransomware.live, „*Belgian Victims of DragonForce*", https://www.ransomware.live/id/UGVyc3luQGRyYWdvbmZvcmNl, 16 April 2026.
51. Ransomware.live, "*Ransomware Statistics for Group: Dragonforce*", https://www.ransomware.live/groupstats/dragonforce, 11 March 2026.
52. ReliaQuest, "*Threat Spotlight: ShinyHunters Targets Salesforce Amid Clues of Scattered Spider Collaboration*", https://reliaquest.com/blog/threat-spotlight-shinyhunters-data-breach-targets-salesforce-amid-scattered-spider-collaboration, 15 September 2025.

53. Resecurity, "*DragonForce Ransomware - Reverse Engineering Report*", https://www.resecurity.com/blog/article/dragonforce-ransomware-reverse-engineering-report, 3 March 2025.
54. SC Media, "*DragonForce ransomware claims denied by Palau*", https://www.scworld.com/brief/dragonforce-ransomware-claims-denied-by-palau, 9 April 2024.
55. SOCRadar, *„Dark Web Profile: DragonForce Ransomware",* https://socradar.io/blog/dark-web-profile-dragonforce-ransomware/, 12 May 2025
56. Sophos, "*DragonForce actors target SimpleHelp vulnerabilities to attack MSP, customers*", https://www.sophos.com/en-us/blog/dragonforce-actors-target-simplehelp-vulnerabilities-to-attack-msp-customers, 27 May 2025.
57. Sophos, *„Nearly Half of Companies Opt to Pay the Ransom, Sophos Report Finds",* https://www.sophos.com/en-us/press/press-releases/2025/06/nearly-half-companies-opt-pay-ransom-sophos-report-finds, 24 May 2025.
58. Sophos, *„The State of Ransomware in Manufacturing and Production 2025*", https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-manufacturing-and-production-2025, 3 December 2025.
59. Specops "*DragonForce: Inside the Ransomware-as-a-Service group*", https://specopssoft.com/blog/dragonforce-ransomware-as-a-service/, 11 November 2025.
60. The Hacker News, "*LockBit, Qilin, and DragonForce Join Forces to Dominate the Ransomware Ecosystem*", https://thehackernews.com/2025/10/lockbit-qilin-and-dragonforce-join.html, 8 October 2025.
61. The Hacker News, *„RansomHub Went Dark April 1; Affiliates Fled to Qilin, DragonForce Claimed Control*", https://thehackernews.com/2025/04/ransomhub-went-dark-april-1-affiliates.html, 30 April 2025.
62. The Raven File, *"Uncovering ALVIVA HOLDING: Links to Russian Shell Companies and Cybercrime"*, https://theravenfile.com/2025/09/08/uncovering-alviva-holding-links-to-russian-shell-companies-and-cybercrime/, 8 September 2025.
63. The Register, "*Here's what we know about the DragonForce ransomware that hit Marks & Spencer*", https://www.theregister.com/2025/05/15/dragonforce_ransomware_uk_retail_attacks/, 15 May 2025.
64. Trend Micro, "*DragonForce"*, https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-dragonforce, 29 October 2025.
65. World Bank Group, "*GDP (current US$)",* https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?view=map, 19 March 2026.
66. World Economic Forum, *„Global Cybersecurity Outlook 2025*", https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf, 13 January 2025.
67. Zensec, *"How RMM abuse fuelled Medusa & DragonForce attacks"*, https://zensec.co.uk/blog/how-rmm-abuse-fuelled-medusa-dragonforce-attacks/, 30 October 2025.

APPENDICES

Appendix A: Indicators of Compromise (IOC Package)

A dedicated MISP event related to this report has been created and shared. It is uniquely identified by UUID as: 3a82cce4-3a41-4abf-9b1d-8ccbdd58f4eb.

Access to the CCB MISP instance can be requested by contacting info@ccb.belgium.be. Requests should indicate whether the intention is to establish a server-to-server connection or to obtain a read-only account on the CCB MISP instance. Read more here about how to access CCB's MISP instance.

Appendix B: Ransom Note

This appendix contains a sample of ransom note left by DragonForce.

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: 1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20

--- 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 8: Sample of ransom note.

Appendix C: Tactics, Techniques, and Procedures (TTP)

This appendix contains the MITRE[55] techniques used by DragonForce.

Tactic	Technique ID	Technique name
Reconnaissance	T1595.002	Active Scanning: Vulnerability Scanning
Resource Development	T1588	Obtain Capabilities
Initial Access	T1189	Drive-by Compromise
	T1190	Exploit Public-Facing Application
	T1133	External Remote Services
	T1566	Phishing
	T1199	Trusted Relationship
	T1078	Valid Accounts
	T1078.002	Valid Accounts: Domain Accounts
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
	T1574.001	Hijack Execution Flow: DLL
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1204	User Execution
	T1204.002	User Execution: Malicious File
Persistence	T1053.005	Scheduled Task/Job: Scheduled Task
	T1112	Modify Registry
	T1078	Valid Accounts
	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
	T1543.003	Create or Modify System Process: Windows Service
Privilege Escalation	T1543.003	Create or Modify System Process: Windows Service
	T1134	Access Token Manipulation
	T1068	Exploitation for Privilege Escalation
Defence Evasion	T1562	Impair Defenses
	T1562.001	Impair Defenses: Disable or Modify Tools
	T1070	Indicator Removal
	T1070.001	Indicator Removal: Clear Windows Event Logs
	T1027	Obfuscated Files or Information
	T1497	Virtualization/Sandbox Evasion
	T1070.006	Indicator Removal: Timestomp
	T1070.004	Indicator Removal: File Deletion
Credential Access	T1003	OS Credential Dumping
	T1555	Credentials from Password Stores
	T1555.003	Credentials from Password Stores: Credentials from Web Browsers
	T1003.001	OS Credential Dumping: LSASS Memory

[55] MITRE ATT&CK, "*Enterprise Matrix*", https://attack.mitre.org/matrices/enterprise/, 18 March 2026.

	T1003.002	OS Credential Dumping: Security Account Manager
Discovery	T1087	Account Discovery
	T1010	Application Window Discovery
	T1518	Software Discovery
	T1482	Domain Trust Discovery
	T1069.002	Permission Groups Discovery: Domain Groups
	T1083	File and Directory Discovery
	T1018	Remote System Discovery
	T1082	System Information Discovery
	T1016	System Network Configuration Discovery
Lateral Movement	T1021	Remote Services
	T1021.001	Remote Services: Remote Desktop Protocol
	T1569.002	System Services: Service Execution
	T1047	Windows Management Instrumentation (WMI)
	T1021.002	Remote Services: SMB/Windows Admin Shares
Collection	T1560	Archive Collected Data
	T1074	Data Staged
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
	T1219	Remote Access Tools
	T1105	Ingress Tool Transfer
Exfiltration	T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage
	T1041	Exfiltration Over C2 Channel
	T1048	Exfiltration Over Alternative Protocol
Impact	T1486	Data Encrypted for Impact
	T1657	Financial Theft
	T1490	Inhibit System Recovery

Figure 9: Tactics, Techniques, and Procedures employed by DragonForce.

Appendix D: Malware & Tools

This appendix contains a set of tools used by the DragonForce.

Name	Description
Mimikatz	A post-exploitation tool used to extract plaintext passwords, hashes, and Kerberos tickets from memory.
LaZagne	An open-source tool for recovering stored credentials from browsers, databases, and other applications.
AdFind / ADFind	A command-line tool used to query Active Directory for reconnaissance and enumeration.
Netscanold.exe	A network scanning utility (often renamed) used by attackers to discover hosts and services.
PassView	A family of tools (e.g., WebBrowserPassView) used to recover saved passwords from various applications.
PCHunter	A tool used for advanced system inspection and kernel-level manipulation, sometimes abused to disable security controls.
ProcessHacker	A powerful process viewer used to inspect, manipulate, or terminate system processes.
MEGA / HTTP / FTP / SFTP	Legitimate file transfer and cloud storage services abused for data exfiltration or payload delivery.
PSExec	A Sysinternals tool used for remote command execution on Windows systems.
RDP (Remote Desktop Protocol)	A built-in Windows feature used for remote access, often abused for lateral movement.
Cobalt Strike	A commercial penetration testing framework widely abused by attackers for command-and-control operations.
SystemBC	A malware proxy/backdoor used to establish persistence and route traffic through compromised systems.
SoftPerfect	Network scanning and administration tools that can be used for reconnaissance inside compromised networks.
SimpleHelp RMM	A Simple RMM is a platform that enables IT teams to remotely monitor systems, automate tasks, and manage endpoints across environments.

Figure 10: Tools employed by DragonForce.