The Godfather of Ransomware? Inside DragonForce's Cartel Ambitions

By Mark Tsipershtein and Evgeny Ananin

Published: 2026-02-03 · Archived: 2026-04-05 16:27:26 UTC

February 03, 2026 8 Minute Read

The Cybereason, A LevelBlue Company, Threat Intelligence Team conducted an analysis of DragonForce, a ransomware group that emerged in late 2023 as a significant cyber threat actor.

DragonForce employs advanced methodologies, using a dual-extortion strategy in which they not only encrypt critical business data but also exfiltrate sensitive information, threatening to release it on dark web leak sites unless the ransom is paid.

DragonForce has targeted a variety of sectors, with a notable focus on manufacturing and construction, and has impacted several high-profile organizations. The group has shown adaptability by continuously refining its tools and tactics, moving from dedicated victim sites to a centralized domain for hosting leaked data. This rapid evolution keeps them a persistent and growing threat to businesses worldwide.

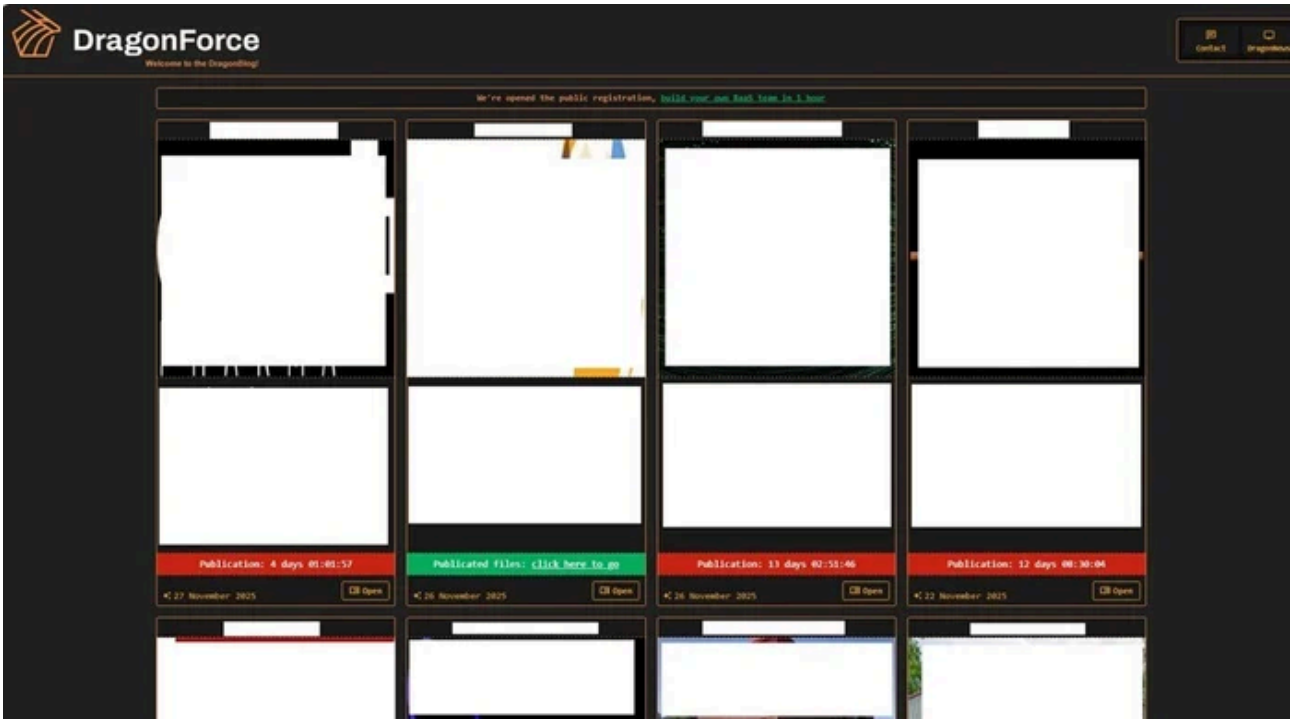


Figure 1. DragonForce's data leak site (DLS).

Key Points

- **Advanced Ransomware Features and Multi-Platform Support:** DragonForce provides a highly flexible ransomware-as-a-service (RaaS) platform that supports various encryption modes, including full, header,

and partial encryption, across multiple platforms, including Windows, Linux, ESXi, and NAS systems.

Its key features include customizable encryption modes for individual files anddelayed-start options for launching attacks. Additionally, the service supports multithreading to improve performance, detailed logging to track the encryption process, and a dry-run option to test the attack without performing actual encryption.

- **New Strategic Direction for DragonForce Ransomware Cartel**: DragonForce has announced a shift in its operational model, now allowing affiliates to create their own brands under the DragonForce ransomware cartel umbrella. This new direction enables affiliates to run its own "projects," offering more autonomy, while still benefiting from the cartel's infrastructure and experience. The cartel is currently in a global update mode, signaling changes to their operational strategies and potentially an expanded network of affiliates. This move reflects the cartel's evolving approach to scaling its ransomware operations.
- **Top Targeted Sectors and Countries by DragonForce**: DragonForce has primarily targeted the manufacturing, business services, technology, and construction sectors. The group’s attacks have been most prevalent in the US, UK, Germany, Australia, and Italy. These industries and countries represent the highest concentration of DragonForce's ransomware activities.

DragonForce Ransomware-as-a-Service

DragonForce Ransomware-as-a-Service (RaaS) Program Overview

The DragonForce RaaS program provides a comprehensive suite of services and tools for cybercriminal affiliates, enabling them to conduct ransomware attacks across a variety of platforms, including Windows, Linux, ESXi, BSD, and NAS systems.

The program promises complete automation of all processes, including file encryption, server management, and attack execution.

It is designed to be highly flexible, supporting full, header, and partial encryption modes, customizable encryption options for individual files, delayed starts, and both local and network modes.

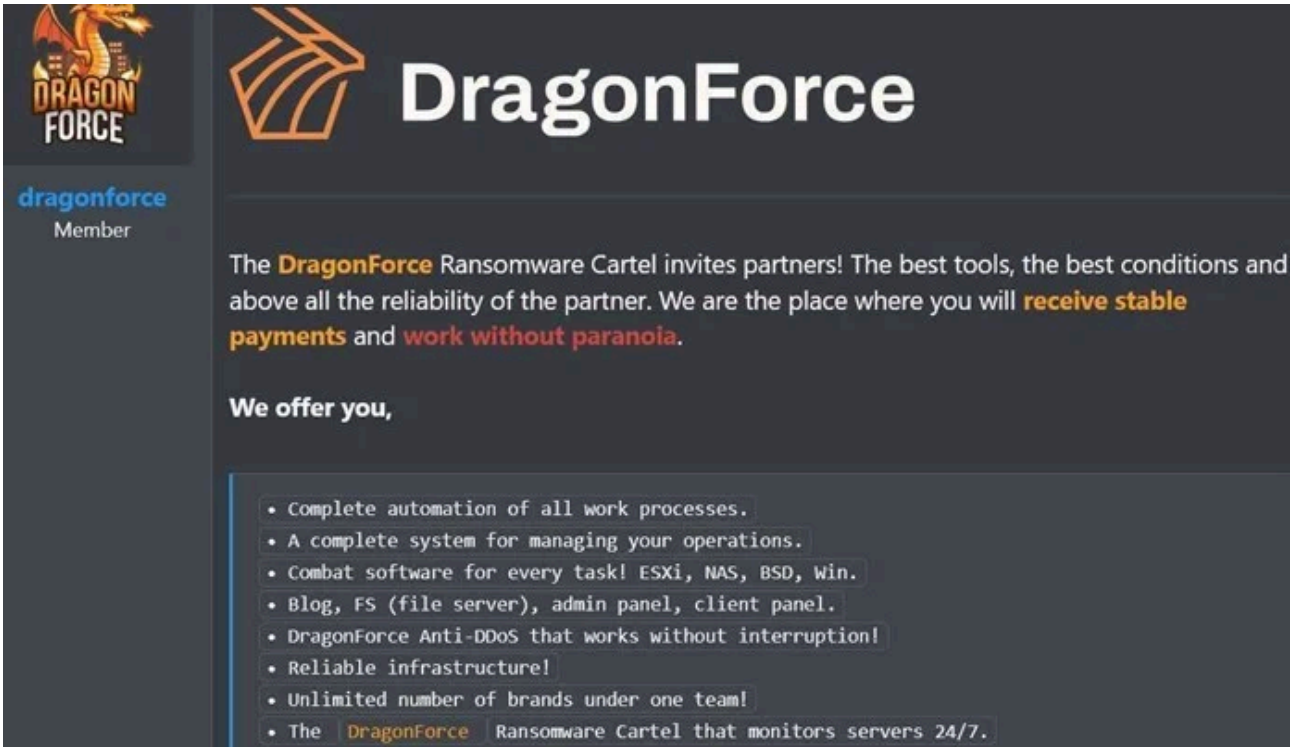


Figure 2. DragonForce's list of key features posted on a dark web forum.

Key features of the program include:

- Unlimited number of brands within one team, allowing affiliates to operate independently.
- PETABYTES of storage, with a dedicated infrastructure for monitoring servers 24/7.
- Free partner services, which include professional file analysis, decryption of complex hashes, and dedicated storage space for affiliates' files.
- Multithreading capabilities to improve performance and detailed logging for tracking encryption progress.
- The option to perform ransomware dry runs without actual encryption, helping affiliates test attacks before deployment.
- The service also supports cross-platform encryption for a wide range of operating systems, ensuring that DragonForce can scale its attacks to diverse environments.

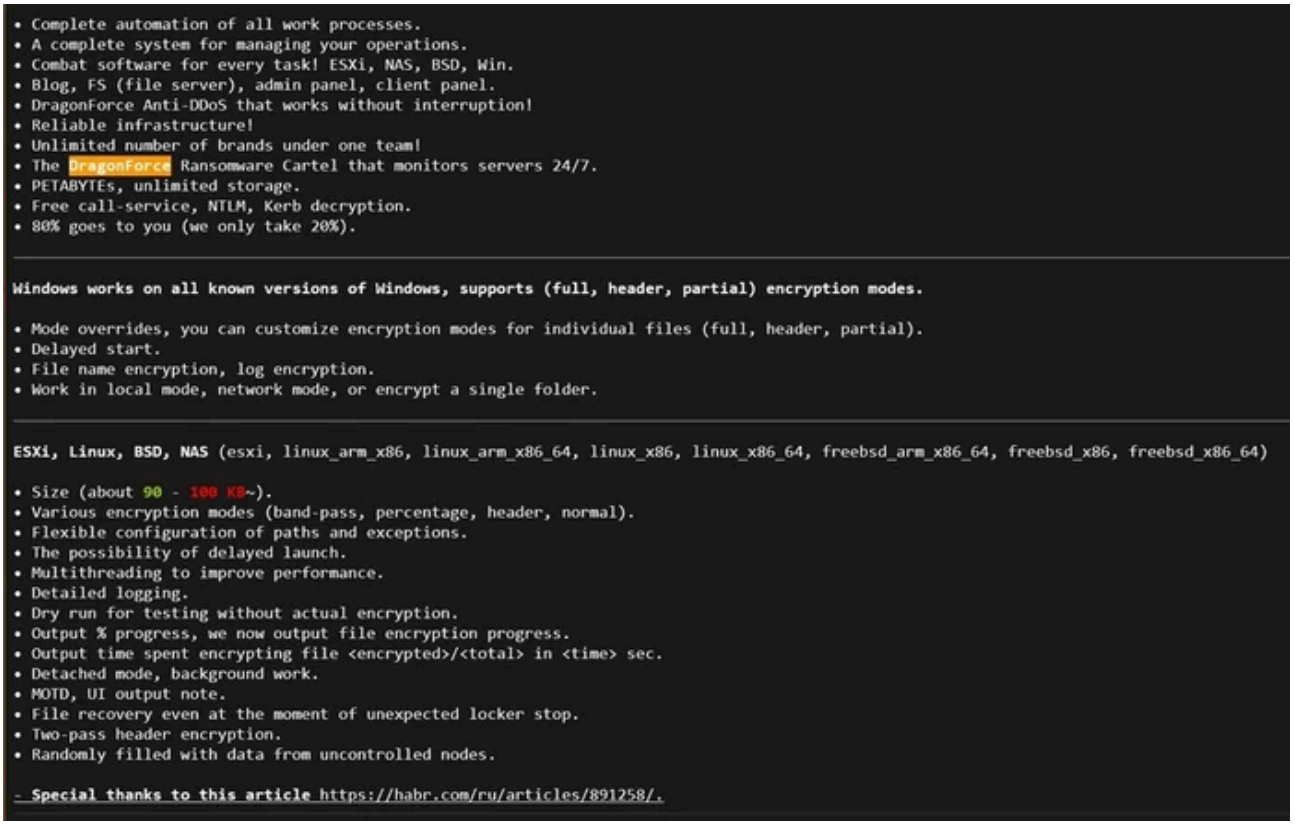
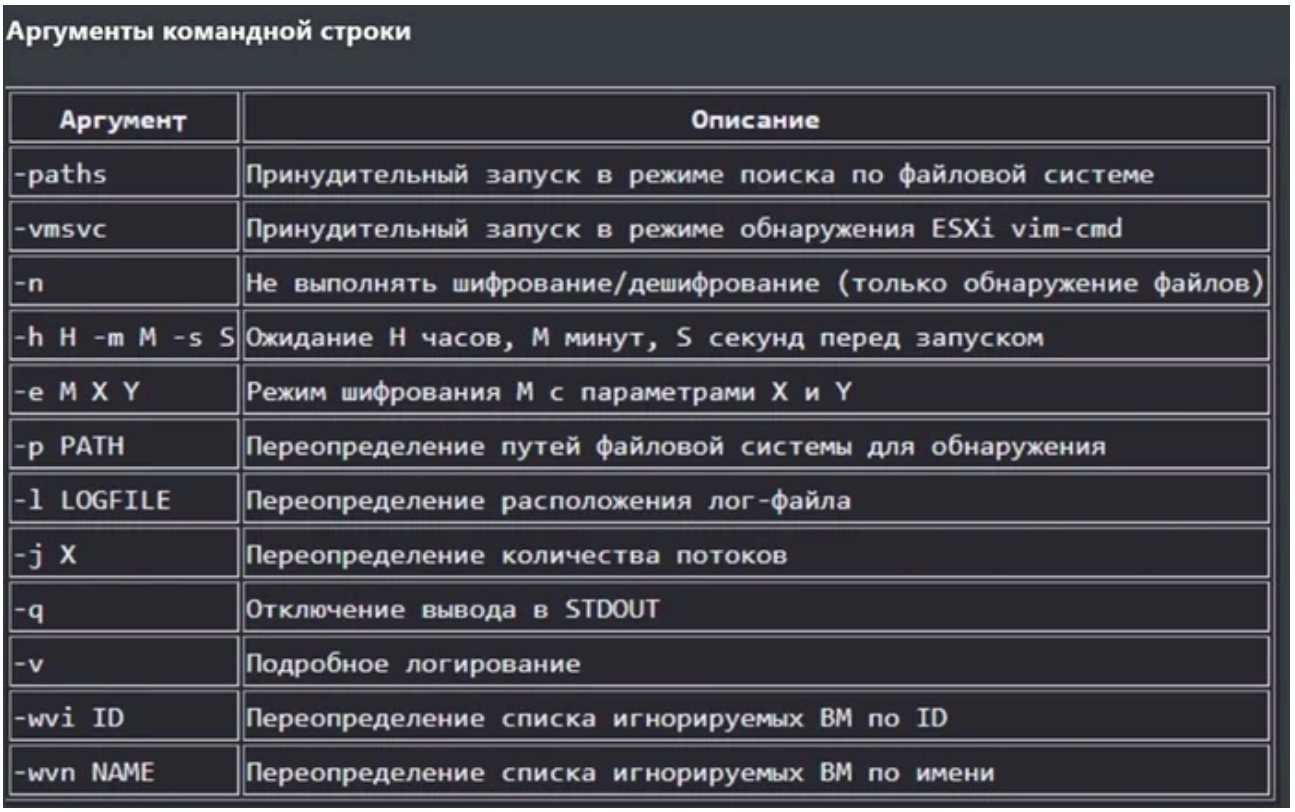


Figure 3. A post on detailing how DragonForce works on Windows, ESXi, Linux, BSD, and NAS.



Аргументы командной строки

Аргумент	Описание
-paths	Принудительный запуск в режиме поиска по файловой системе
-vmsvc	Принудительный запуск в режиме обнаружения ESXi vim-cmd
-n	Не выполнять шифрование/дешифрование (только обнаружение файлов)
-h H -m M -s S	Ожидание H часов, M минут, S секунд перед запуском
-e M X Y	Режим шифрования M с параметрами X и Y
-p PATH	Переопределение путей файловой системы для обнаружения
-l LOGFILE	Переопределение расположения лог-файла
-j X	Переопределение количества потоков
-q	Отключение вывода в STDOUT
-v	Подробное логирование
-wvi ID	Переопределение списка игнорируемых ВМ по ID
-wvn NAME	Переопределение списка игнорируемых ВМ по имени

Figure 4. DragonForce's ESXi encrypter command-line options.

Command-Line Arguments:

-paths: Enforces search mode in the file system.

-vmsvc: Forces search in the ESXi detection mode using vim-cmd.

-n: Do not perform encryption/decryption (only file detection).

-h H -m M -s S: Wait H hours, M minutes, and S seconds before starting.

-e M X Y: Encryption mode with parameters M, X, and Y.

-p PATH: Redefines the file system paths for detection.

-l LOGFILE: Redefines the log file location.

-j X: Redefines the number of threads to use.

-q: Disables output to STDOUT.

-v: Enables detailed logging.

-wvi ID: Redefines the list of ignored BMs by ID.

-wv NAME: Redefines the list of ignored BMs by name.

Figure 5. DragonForce's ESXi encrypter configuration options

Configuration File Options:

- dry_run: Mode without actual encryption/decryption (for testing purposes).
- encryption.extension: Defines the file extension for encrypted files.
- encryption.rename: Renames encrypted files.
- encryption.mode: Specifies the encryption mode (options: striped, percent, header, normal).
- encryption.p1, encryption.p2: Parameters for encryption mode.
- work_mode: Specifies the working mode (options: vmsvc, paths).
- paths: Paths for encrypting files.
- note_file: Name of the file that stores the ransom note.
- log.file: Path to the log file.
- log.encrypted: Enables encryption logging.
- delay: Delay before starting the encryption process (in seconds).
- whitelist.paths: Directories to be excluded from encryption.

- whitelist.extensions: File extensions to be excluded from encryption.
- whitelist.filenames: Specific file names to be excluded from encryption.
- whitelist.vm_ids: Virtual machine IDs to be excluded from encryption.
- whitelist.vm_names: Virtual machine names to be excluded from encryption.

Figure 6. Ransomware client builder.

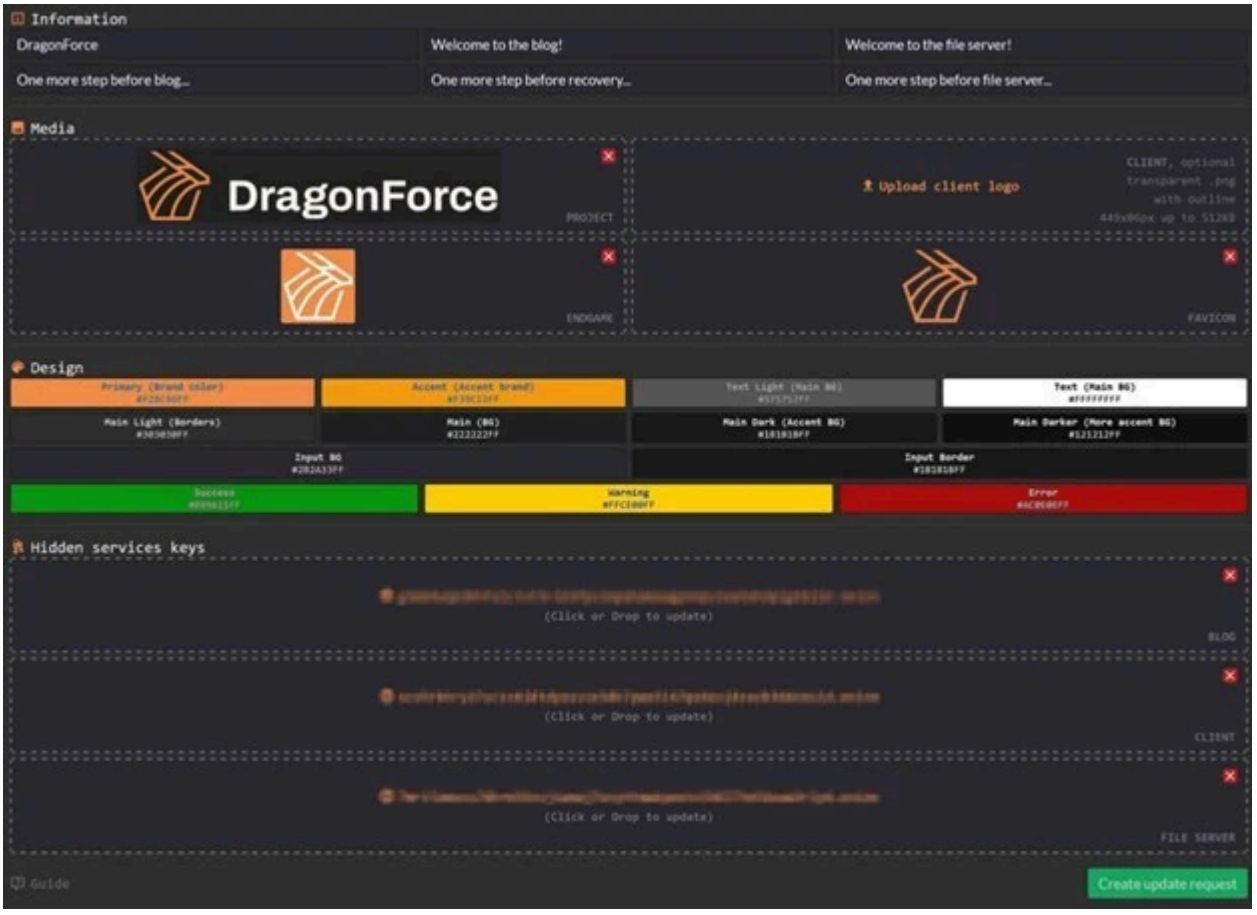


Figure 7. Configuration interface.

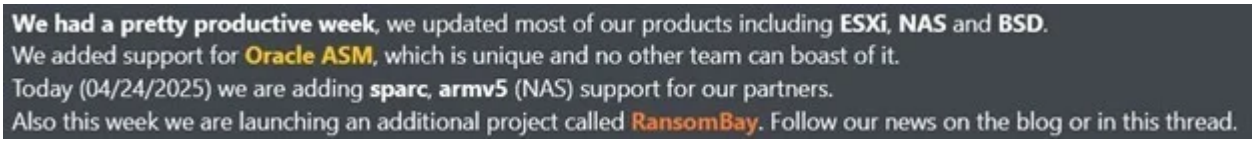


Figure 8. DragonForce announced support for Oracle ASM and project RansomBay.

Figure 9. DragonForce'sRansomBay project.

DragonForce has recently created an automated registration service for those interested in joining its ransomware operations. This change allows new affiliates to register directly without prior approval or extensive vetting, unlike previous practices that required a significant monetary deposit and detailed background checks.

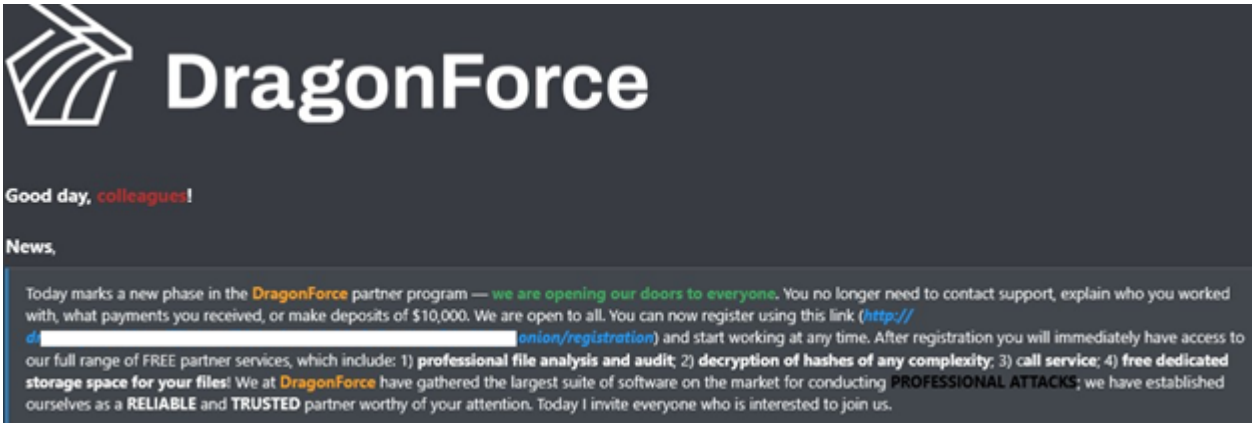


Figure 10.

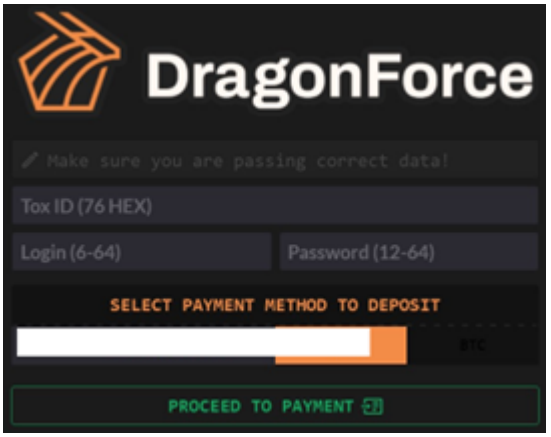


Figure 11. DragonForce's automated registration system.

Figure 12. An advertisement of DragonForce's new automated registration system.

DragonForce also announced that its upcoming "product", DragonForce - Atom, will be released soon. Unfortunately, the group has not published the details yet on the new product.

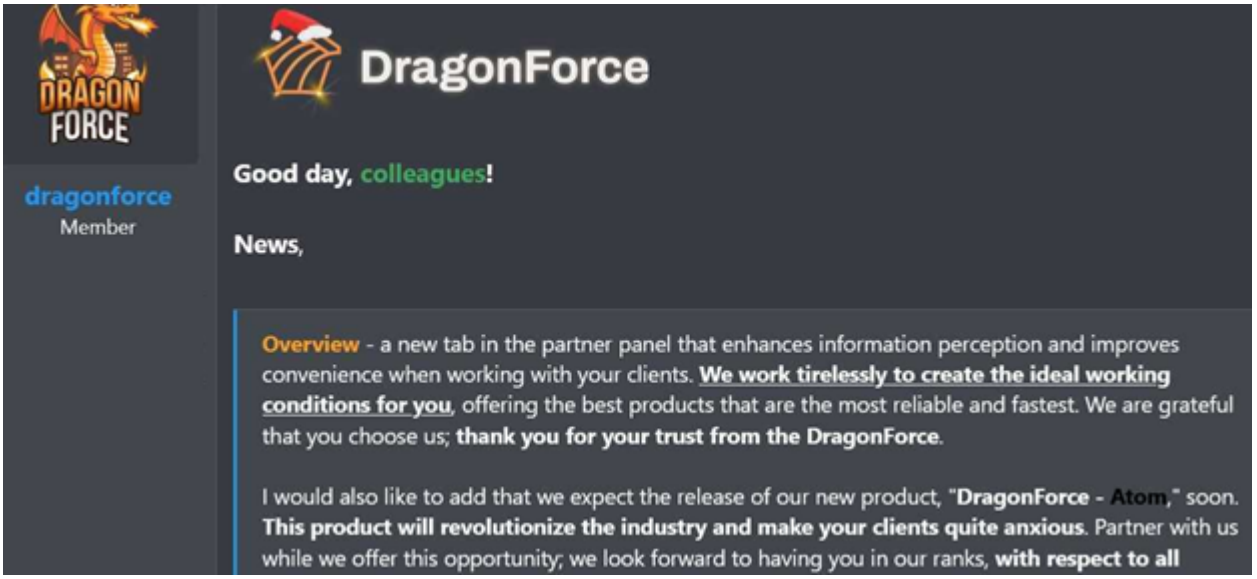


Figure 13. DragonForce's announcement of its new DragonForce – Atom product.

Professionalization of Ransomware Operations Through Data Audits

Rather than advertising malware or access, DragonForce created the “Company Data Audit” service to support ransomware affiliates during extortion campaigns. The service is positioned as complementary to decryption and negotiation support, with the stated goal of strengthening leverage over victims by analyzing stolen data and clearly articulating business, legal, and reputational risks.

The audit includes a detailed risk report, prepared communication materials, such as call scripts and executive-level letters, and strategic guidance designed to influence negotiations. An example provided references a mining company breach in which stolen satellite imagery allegedly exposed sensitive mineral deposit locations, illustrating the group’s emphasis on extracting strategic and non-obvious value from exfiltrated data. The service is offered under a commission-based model, with higher percentages charged for post-incident or “historical” cases.

Overall, the content highlights the continued professionalization of ransomware operations and the expansion of their supporting ecosystems. It reflects a shift toward intelligence-driven extortion, where threat actors invest in data analysis, tailored messaging, and negotiation strategy to maximize ransom outcomes, mirroring legitimate consulting and risk assessment practices.

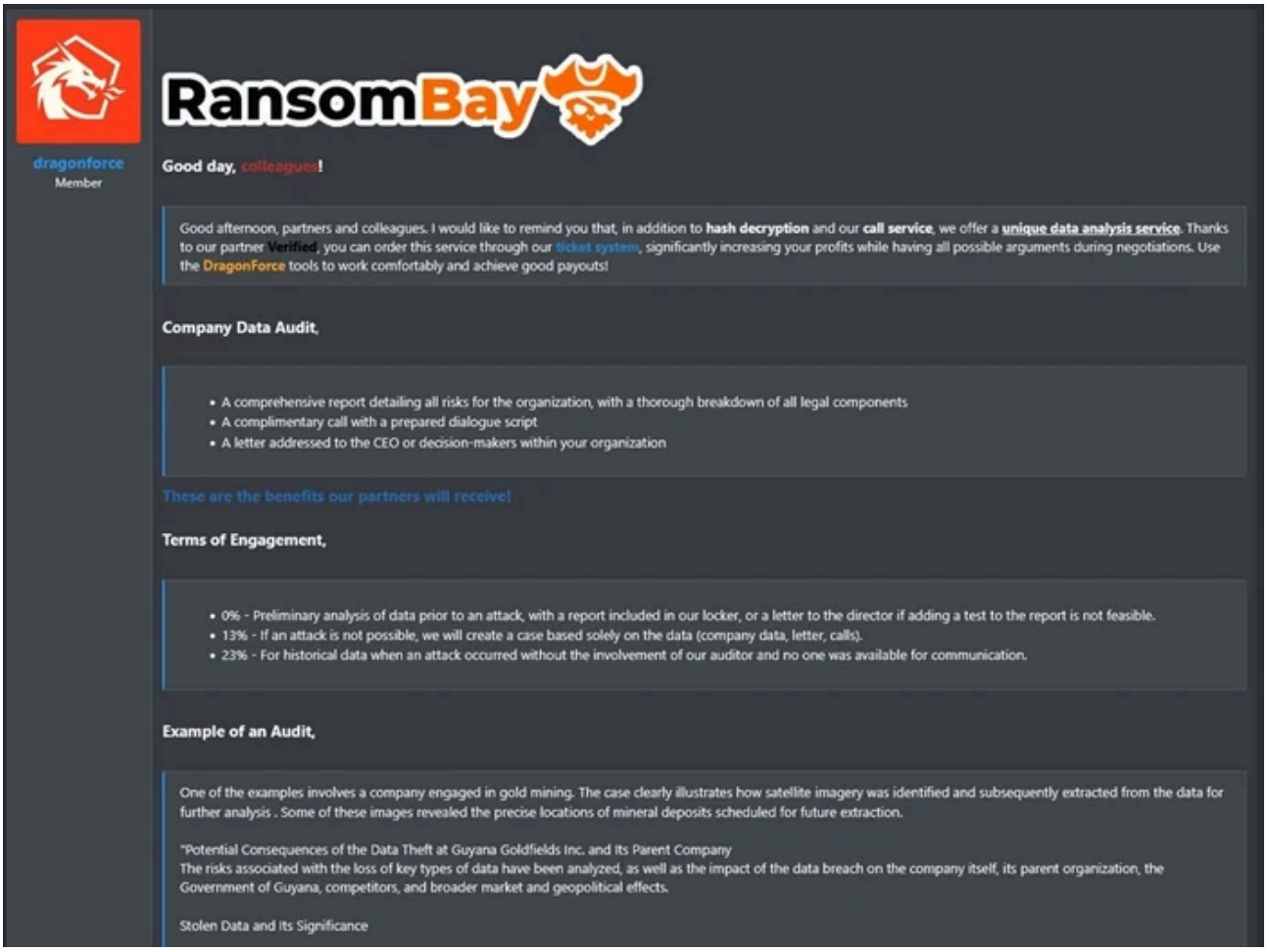


Figure 14. DragonForce promotes a value-added service offered by threat actors associated with the DragonForce ransomware ecosystem.

DragonForce Vs RansomHub

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.

The group then turned its attention to RansomHub, whose infrastructure went offline on April 1, 2025. DragonForce claimed RansomHub had joined the cartel and even created a dedicated portal for former RansomHub affiliates migrating and adopting the DragonForce branding. RansomHub pushed back publicly, with spokesperson Koley accusing DragonForce of sabotage, internal betrayal, and even cooperating with law enforcement.

Figure 15. DragonForce claimed RansomHub had joined the cartel and even created a dedicated portal for its affiliates.

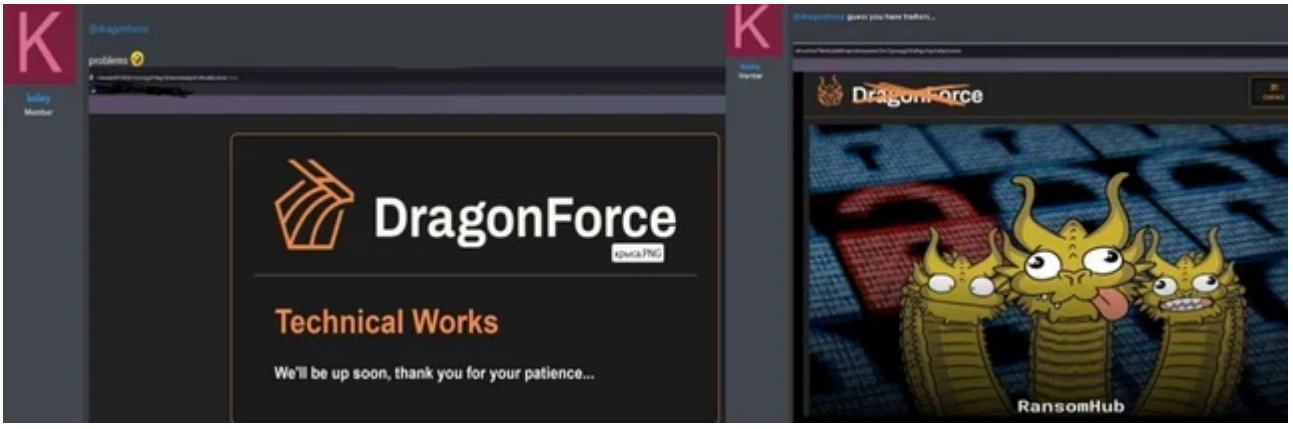


Figure 16. RansomHub publicly denied that it joined DragonForce.

As part of the escalating conflict between DragonForce and RansomHub, a RansomHub spokesperson publicly accused DragonForce of having contacts within the Russian FSB intelligence service, implying that DragonForce leveraged these connections to undermine or sabotage rival ransomware groups.

DragonForce also targeted the BlackLock ransomware group by defacing its leak site:

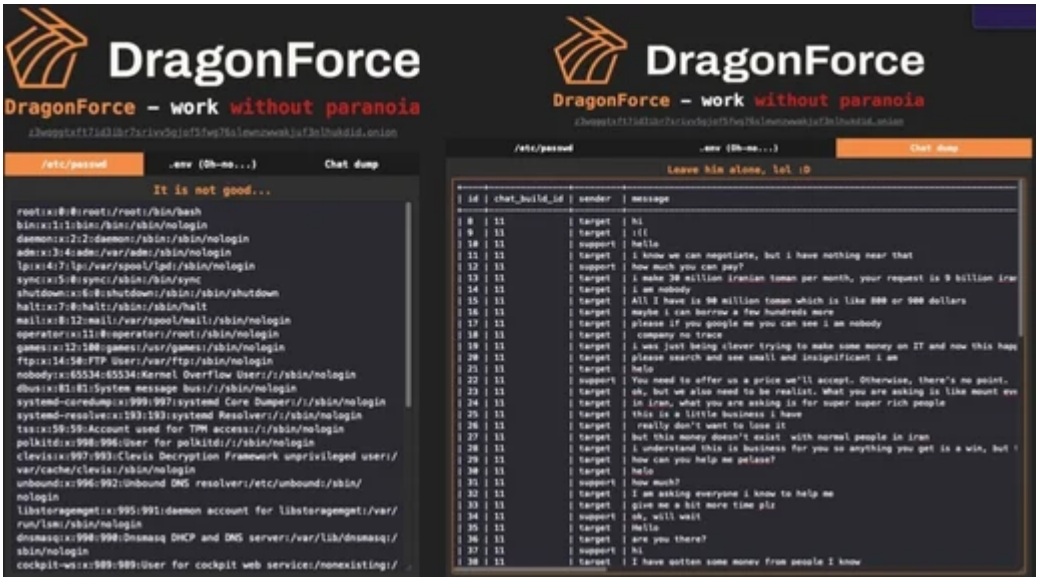


Figure 17. DragonForce defaced the RansomLock ransomware group's DLS.

Formation of a Cybercrime Cartel

Cybereason's threat intelligence team has information that a representative of the DragonForce ransomware group issued an open call for cooperation among major ransomware operations, explicitly naming LockBit and Qilin. There is also evidence that Nova RaaS group representatives participated in this initiative.

The DragonForce representative's message proposed establishing communication channels between groups, standardizing competitive conditions, and eliminating public conflicts. The author advocated for mutually agreed-upon rules, including equal terms for affiliates, no undercutting of deposit or profit-share percentages, and maintaining a professional level of conduct. The stated objective is to stabilize the ransomware "market," increase collective profits, and present a unified front.

Shortly after issuing its public call for cooperation, DragonForce released an official statement announcing the formation of a "coalition" between Qilin, LockBit, and DragonForce.

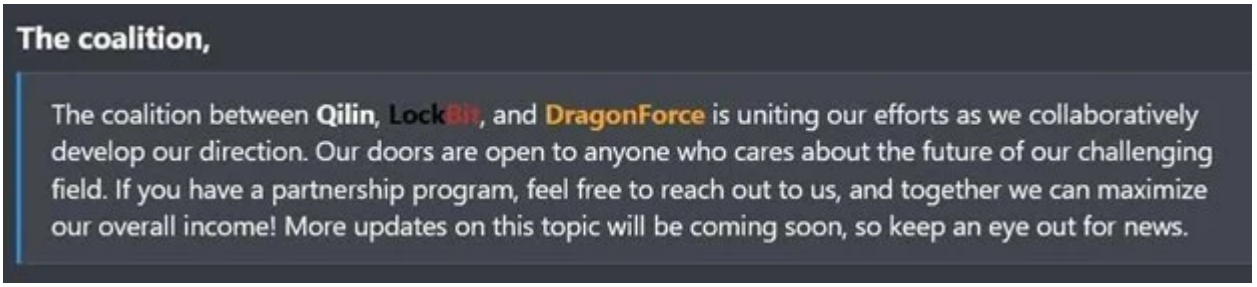


Figure 18. A post announcing the formation of a coalition between Qilin, LockBit, and DragonForce.

DragonForce Or DragonForce?

Claims alleging a relationship between DragonForce Malaysia and the DragonForce ransomware group remain unsubstantiated. On October 28, 2025, DragonForce Malaysia publicly denied any affiliation or involvement with

the DragonForce ransomware operation, stating that such allegations are based on indirect and weak evidence and that ransomware activity is inconsistent with its mission and objectives.

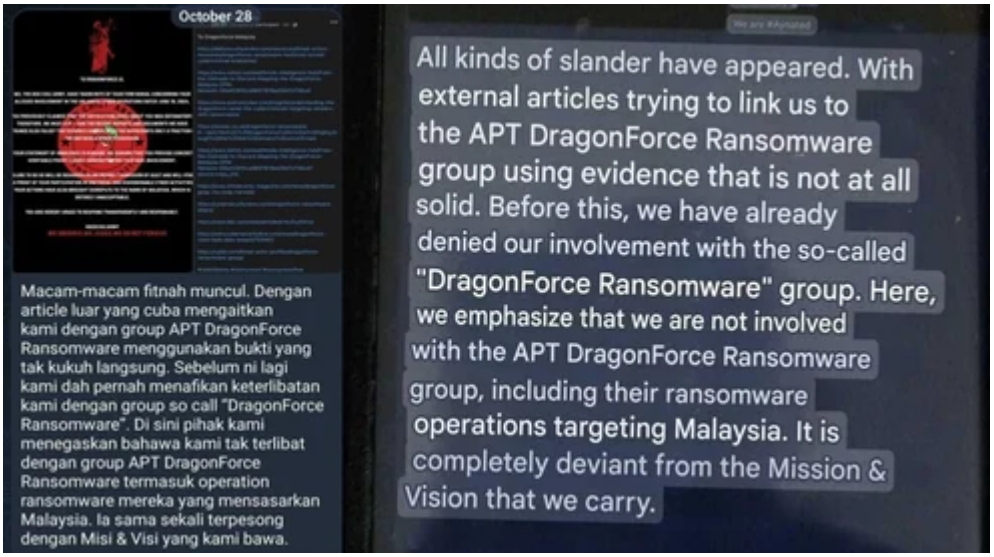


Figure 19. DragonForce Malaysia rejected accusations linking the group to ransomware activities attributed to the DragonForce ransomware/APT cluster.

Figure 20. In the early stages of its operations, the DragonForce ransomware group had a profile on BreachForums.

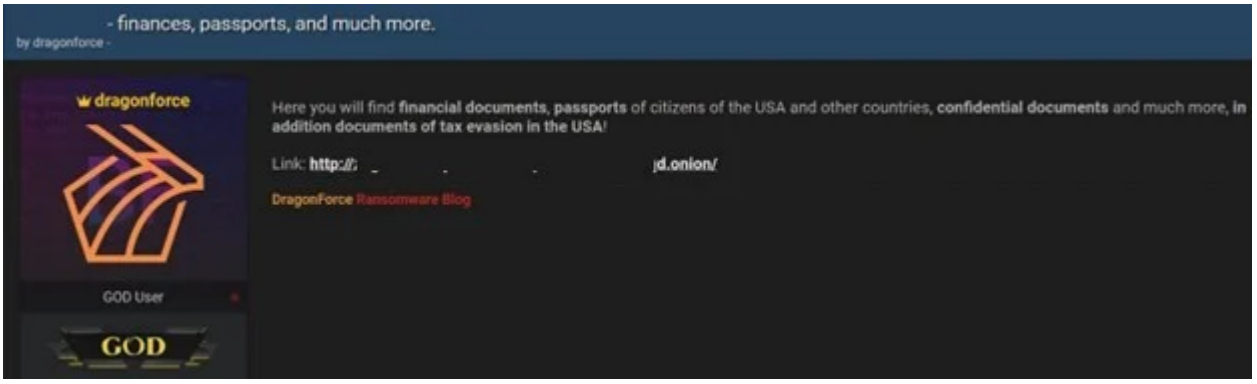


Figure 21. One of the early posts of the user "dragonfoce" on BreachForums.

In a leaked database from BreachForums, it was discovered that a user associated with the DragonForce username had registered using the email address bjorkaact@.

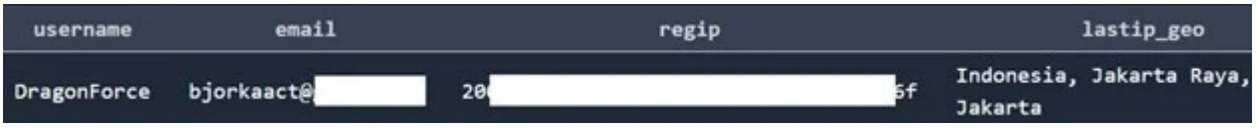


Figure 22. BreachForums leaked data showing the DragonForce username and its associated email address.

Profiles associated with DragonForce have been identified across different versions of BreachForums, each with a different registration date. A user profile from BreachForums version 2 shows a registration in 2023, while a separate leak from BreachForums version 1 reveals a DragonForce profile with a registration date in 2022.

Bjorka is a well-known cyber threat actor alias associated with a string of high-profile data breaches and leaks that first appeared on underground forums like RaidForums and later BreachForums.

Alias Bjorka has been tied to Babuk2 or "Babuk-Bjorka," which emerged in early 2025, while mostly recycling data already leaked by other groups such as RansomHub and FunkSec.

In a January 2026 database leak from a newer version of BreachForums, a user associated with the DragonForce nickname had registered using the email address Albikatoras555[@]protonmail[.]com.

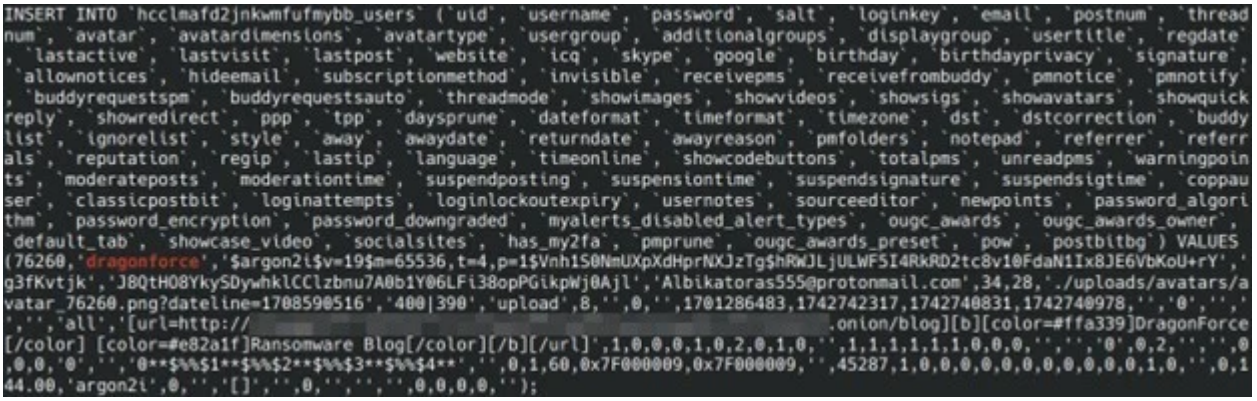


Figure 23. BreachForums 2026 database entry for "dragonforce".

Additionally, OSINT indicates the DragonForce ransomware Onion blog has been associated with a clear-net IP address that appears in FOFA search results as being hosted within infrastructure geolocated to the Russian Federation.

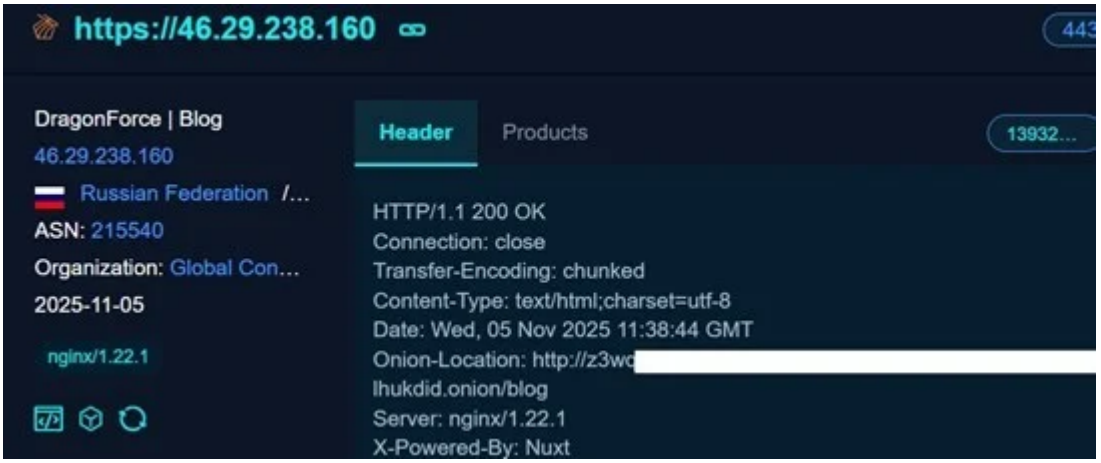


Figure 24. DragonForce's Onion blog FOFA search results.

The IP association was first identified by @RakeshKrish12 and independently confirmed by the Cybereason Threat Intelligence Team.

Currently, the DragonForce group has fixed the IP leak, so the Onion website cannot be easily located on the public Internet.

Figure 25. Let's Encrypt SSL certificate.

Among the other IPs seen hosting the DragonForce infrastructure, we have observed the following IP addresses to be in use:

- 193[.]233.175.213
- 95[.]164.53.64
- 91[.]108.244.85
- 46[.]29.238.160
- 46[.]29.238.123
- 87[.]121.47.15

Technical Analysis

In this section, we performed an analysis of the ransomware executable file and observed similarities in technique with other ransomware groups.

The file hash is as follows:

```
c5554ab2ea04e9d938a47b09ea34ebedb46c223a500aa70f08f4b2dc6864bd90
```

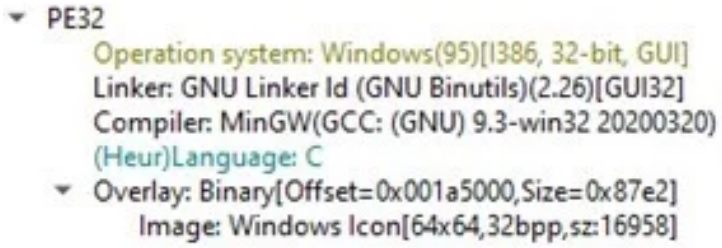


Figure 26. "Detect it Easy" analysis information.

The mutex *hsfjuukjzloqu28oajh727190* is a hardcoded identifier first documented in a ransomware sample derived from the leaked Conti source code, where it was used to ensure only one instance of the malware runs at a time on a victim's machine. This mutex appears in ransomware families known to reuse Conti components, including DragonForce variants.

Figure 27. DragonForce mutex.

The DragonForce ransomware group is known to scan SMB ports within IP ranges during its operations. This scan is part of the group's network reconnaissance activities, used to identify vulnerable systems and potential targets for ransomware deployment.

Figure 28. DragonForce scans local machines for reconnaissance.

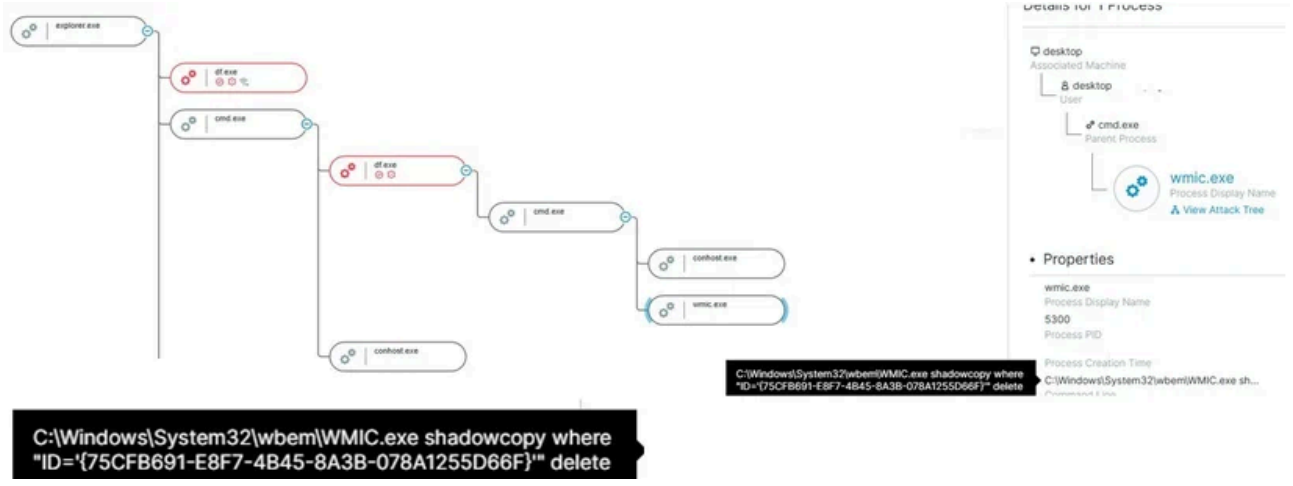
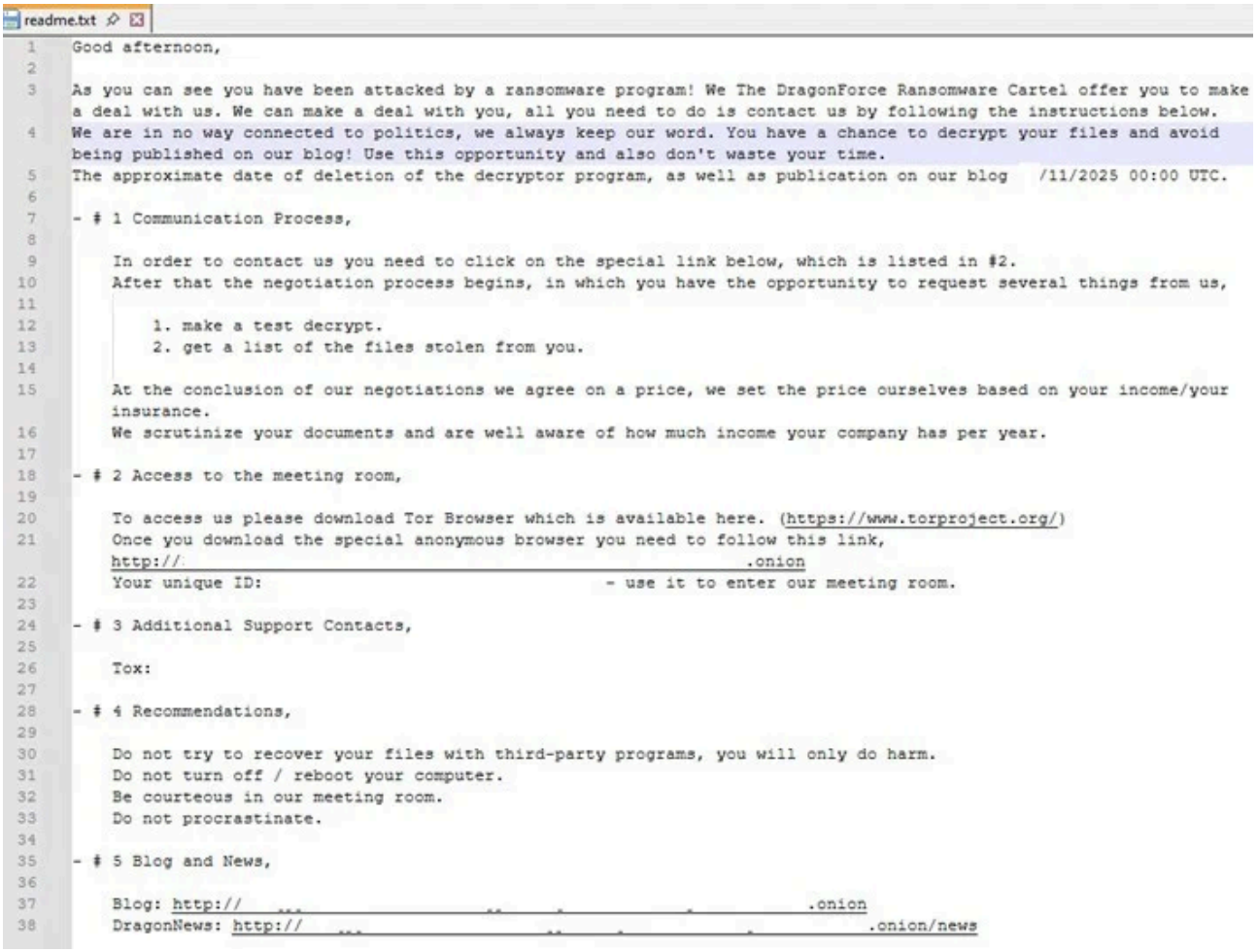


Figure 29. Shadow copy delete via WMIC.

The group utilizes the wmic.exe command with the shadowcopy function, specifically using the command wmic.exe shadowcopy where "ID='{id}'" delete. This command is employed to delete volume shadow copies, which are commonly used by ransomware to erase backup copies of files.

Figure 30. Encrypted files


readme.txt

```
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   /11/2025 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://                                                          .onion
    Your unique ID:                                  - 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://                                                    .onion
    DragonNews: http://                                                    .onion/news
```

Figure 31. DragonForce's ransom note.

The Cybereason platform successfully detected the malicious payload associated with the DragonForce ransomware, identifying and blocking its attempt to delete shadow copies via the wmic.exe command. Additionally, the product detected and prevented the ransomware from encrypting files, ensuring that critical data remained intact and secure.

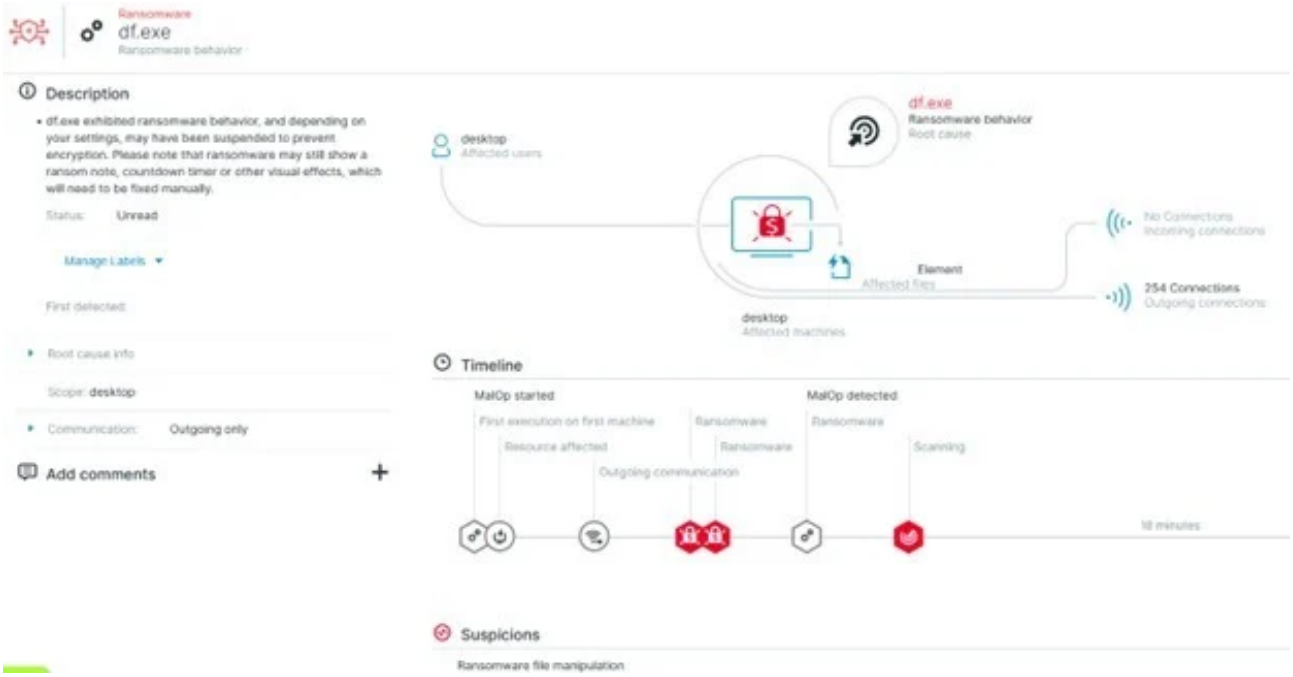


Figure 31. Detection and prevention.

Cybereason's analysis shows that DragonForce is a highly adaptive, rapidly evolving ransomware operation, that combines sophisticated RaaS features, dual-extortion tactics, and cross-platform capabilities (Windows, Linux, ESXi). With its automated persistence mechanisms, flexible propagation methods, and extensive support for affiliates, DragonForce can scale its attacks efficiently and bypass basic defenses. Its swift publication of victim data, powerful encryption, EDR evasion techniques, and lateral movement capabilities make it a persistent and significant threat to organizations, with the potential to disrupt a wide range of industries globally.

Recommendations:

- Follow and hunt "DragonForce" Locker affiliate activity to identify pre-ransomware behaviors
- Promote cybersecurity best practices such as multifactor authentication (MFA) and patch management.
- Regularly back up files and create a backup process and policy: Restoring your files from a backup is the fastest way to regain access to your data
- Keep systems fully patched: Make sure your systems are patched to mitigate vulnerabilities
- If nefarious activity is detected, immediately involve Incident Response services to execute a thorough investigation and containment process to fully eliminate the threat actor from the infected network
- For Cybereason customers on the Cybereason Defense Platform: DragonForce ransomware is detected with the default configuration of the Defense Platform. To ensure detection and effective prevention of DragonForce-related activity, these security features must be enabled:
    - Enable Anti-Malware and set the Anti-Malware Signatures mode to Prevent, Quarantine, or Disinfect.

- Enable Anti-Ransomware (PRP), set Anti-Ransomware to Quarantine mode and enable shadow copy protection
- Enable Application Control
- Enable Variant Payload Prevention with prevent mode on Cybereason Behavioral execution prevention.

IOCs

IOC	IOC type	Description
c5554ab2ea04e9d938a47b09ea34ebedb46c223a500aa70f08f4b2dc6864bd90	SHA256	Windows Ransomware Sample
49e77b75aceac589dd86abf4cc643e5ce4a0e44eed8b39e17e9c8bf768d143ff	SHA256	Windows Ransomware Sample

MITRE ATT&CK Mapping

Tactic	ATT&CK Technique (ID)
Initial Access	Valid Accounts (T1078)
TA0002: Execution	T1059.001 – Command and Scripting Interpreter: PowerShell T1569.002 – System Services: Service Execution
TA0003: Persistence	T1547.001 – Registry Run Keys / Startup Folder T1078.002 – Valid Accounts: Domain Accounts
TA0005: Defense Evasion	T1070.004 – Indicator Removal on Host: File Deletion T1070.001 – Indicator Removal on Host: Clear Windows Event Logs T1562.001 – Impair Defenses: Disable or Modify Security Tools T1562 – Impair Defenses T1222 – File and Directory Permissions Modification T1218 – System Binary Proxy Execution (use of trusted Windows utilities such as wmic)
TA0007: Discovery	T1083 – File and Directory Discovery T1135 – Network Share Discovery T1018 – Remote System Discovery
TA0008: Lateral Movement	T1047 – Windows Management Instrumentation (WMI) T1021.002 – Remote Services: SMB/Windows Admin Shares
TA0040: Impact	T1486 – Data Encrypted for Impact T1489 – Service Stop T1490 – Inhibit System Recovery

---

Source: https://www.levelblue.com/blogs/spiderlabs-blog/the-godfather-of-ransomware-inside-dragonforces-cartel-ambitions