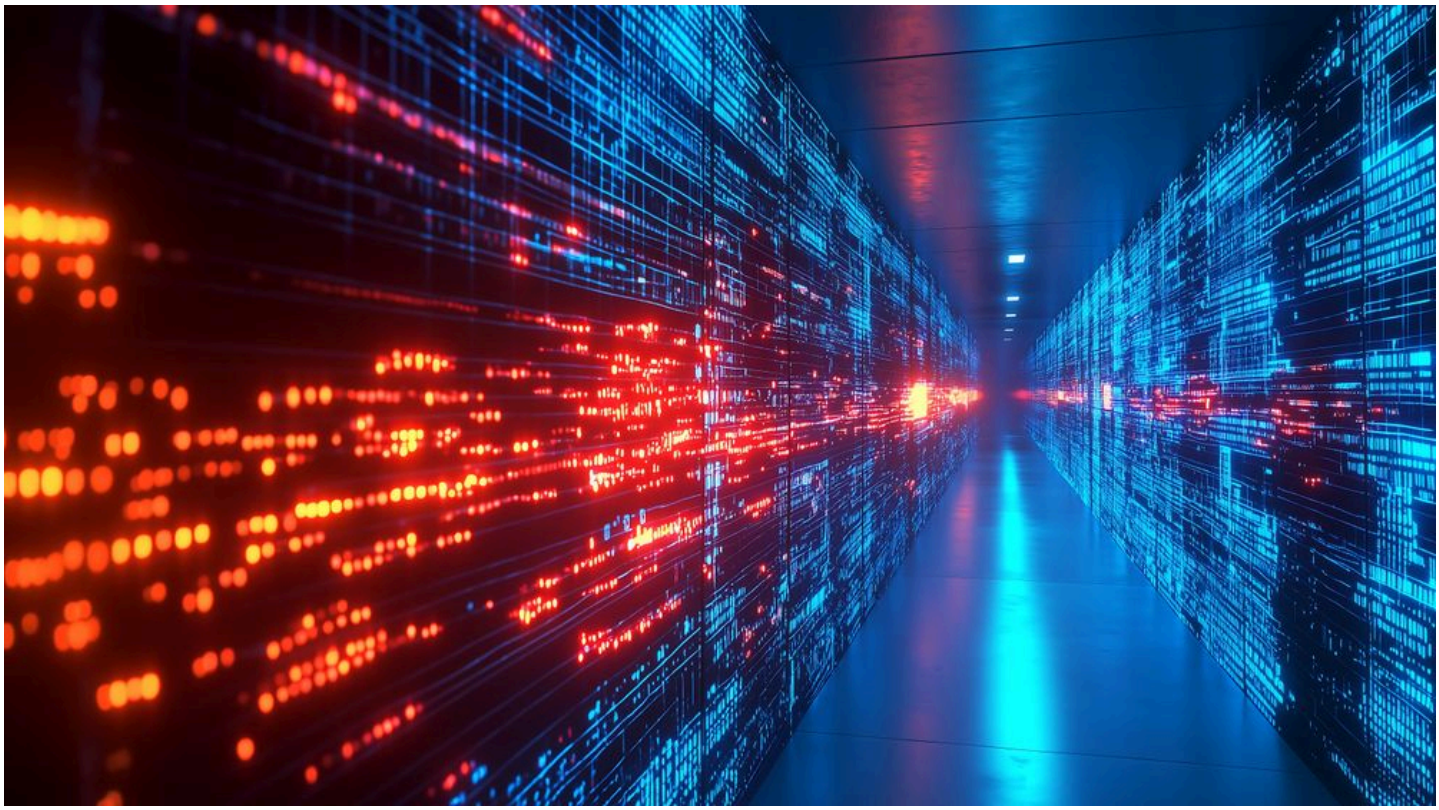
# The DragonForce Cartel: Scattered Spider at the gate



**From Conti's leaked code to alliances with LAPSUS$ and ShinyHunters in The Com ecosystem**

**Authors: Darrel Virtusio, David Catalan Alegre, Eliad Kimhy, Santiago Pontiroli**

## Summary


- Acronis Threat Research Unit (TRU) analyzed DragonForce, a Conti-derived ransomware-as-a-service active since 2023, documenting its malware, affiliate model and links to Scattered Spider.
- DragonForce rebranded as a ransomware cartel, allowing affiliates to white-label payloads and create variants like Devman and Mamona/Global, while defacing rival groups to reinforce its position in the ecosystem.
- DragonForce and LockBit Green share common lineage through the leaked Conti v3 code, leading to overlaps in routines and artifacts.
- DragonForce employs BYOVD (bring your own vulnerable driver) attacks by using truesight.sys and rentdrv2.sys drivers to terminate processes.
- After an article appeared in Habr — a media platform focused on technology, internet culture and related topics — revealed weaknesses in Akira's encryption, DragonForce quickly reinforced its own encryptor to avoid similar problems.

- Scattered Spider, a financially driven actor known for phishing, SIM swapping and MFA bypass, partnered with operators tied to the DragonForce ransomware-as-a-service model. This collaboration evolved into broader overlaps with LAPSUS$ and ShinyHunters, forming what researchers dubbed the “Scattered LAPSUS$ Hunters” within the “Hacker Com” ecosystem.
- More than 200 victims have been exposed on DragonForce’s leak site since late 2023, across retail, airlines, insurance, MSPs and other enterprise sectors.

# Introduction

Acronis Threat Research Unit (TRU) analyzed recent activity linked to the DragonForce ransomware group and identified a new malware variant in the wild. The latest sample uses vulnerable drivers such as truesight.sys and rentdrv2.sys to disable security software, terminate protected processes and correct encryption flaws previously associated with Akira ransomware. The updated encryption scheme addresses weaknesses publicly detailed in a Habr article cited on DragonForce’s leak site.

Recently, DragonForce announced a rebrand, stating that the group would now operate as a cartel. This shift in operation strategy aims to grow their presence in the ransomware scene. By offering affiliates 80 percent of profits, customizable encryptors and infrastructure, DragonForce lowers the barrier to entry and encourages more affiliates to join the cartel. Since then, DragonForce has been more active in attacking companies globally, posting more victims compared to a year ago. Their most notable attack, publicly attributed to the group, targeted retailer Marks & Spencer in collaboration with Scattered Spider.

In this blog we provide an analysis of DragonForce’s new ransomware variant and provide background information on the group’s activities and affiliations.

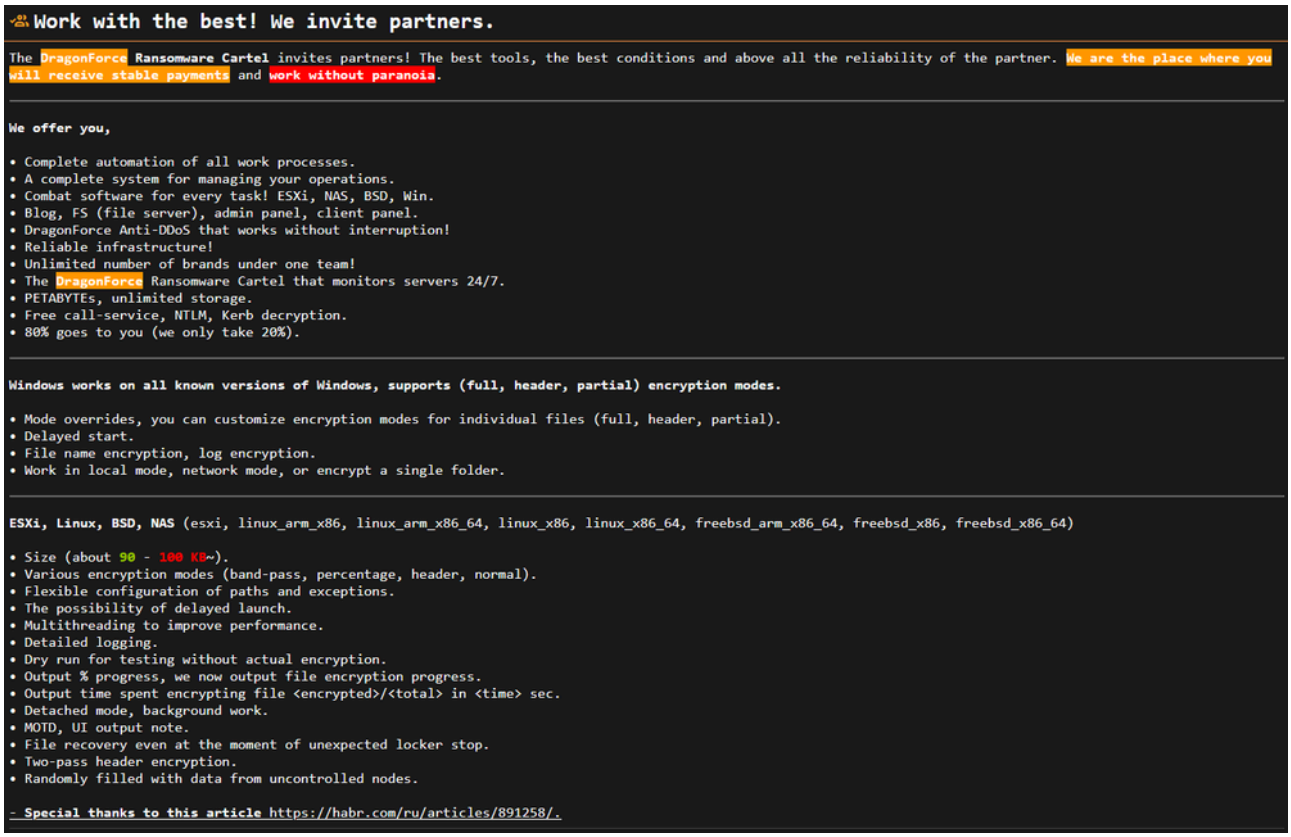
## The rise of DragonForce

DragonForce is a ransomware-as-a-service (RaaS) group that first appeared in 2023 and was initially associated with the hacktivist group DragonForce Malaysia, though concrete evidence linking the two is still limited. Ever since DragonForce entered the ransomware scene, they have been actively recruiting partners on underground forums for its operation. The group started using the leaked LockBit 3.0 builder to develop its encryptors, then later adopted a customized Conti v3 code.

The DragonForce Ransomware Cartel announcement

In early 2025, DragonForce began branding itself as a ransomware “cartel.” This approach allows DragonForce to continue building its brand as one of the most notorious cybercriminal groups currently active, drawing attention from

rivals and law enforcement. Through its affiliate program, DragonForce strengthened its position in the ransomware scene, attracting new partners and competing with more established RaaS operators. Additionally, this business model diversifies techniques and victims, making attribution increasingly difficult.

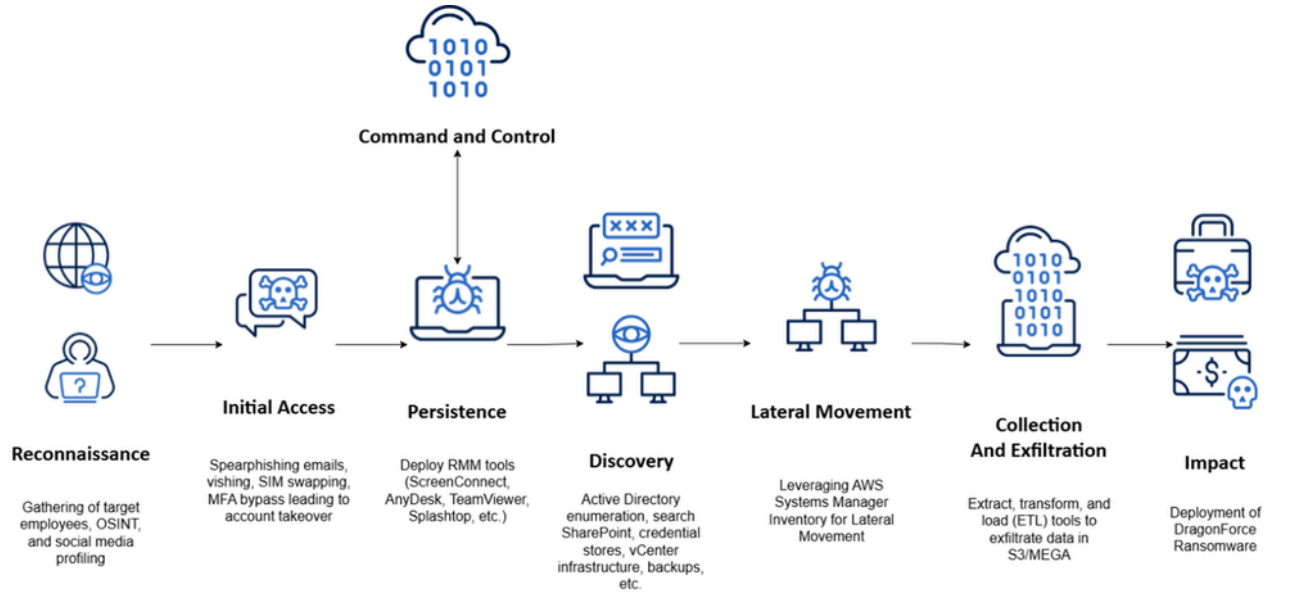


DragonForce advertises its malware on its data leak site

Affiliates can deploy their own malware while using DragonForce's infrastructure and operating under their own brand. This lowers the technical barrier and allows both established groups and new actors to run operations without building a full ransomware ecosystem.

This rebranding created an attractive proposition for both established and emerging groups. Among DragonForce's partners is Scattered Spider, an initial access broker known for collaborating with multiple ransomware operations. The group's campaigns have produced many victims, including well-known organizations such as Marks & Spencer and Harrods.

While the cartelization of cybercriminal groups is not new, it has gained momentum in recent years. Beyond DragonForce, groups like Scattered Spider, LAPSUS$ and ShinyHunters have formed collectives such as Scattered LAPSUS$ Hunters, reportedly behind several high-profile breaches involving Salesforce customers. This shift from competition to collaboration marks a growing risk for organizations worldwide.




Anatomy of DragonForce: Execution chain aligned with MITRE ATT&CK tactics

## How Scattered Spider enables DragonForce ransomware deployments

The intrusion typically involves Scattered Spider identifying their target victims by performing reconnaissance on the organization's employees to create a persona and pretext. They gather victim information such as name, role, and other general information through social media and open-source intelligence methods. The group employs sophisticated social engineering techniques such as spear-phishing emails and voice phishing (vishing) to obtain and / or reset victim credentials and bypass MFA through convincing lures, multifactor authentication fatigue or SIM swaps. Once successful, Scattered Spider logs in as the targeted user and enrolls their own device for access.

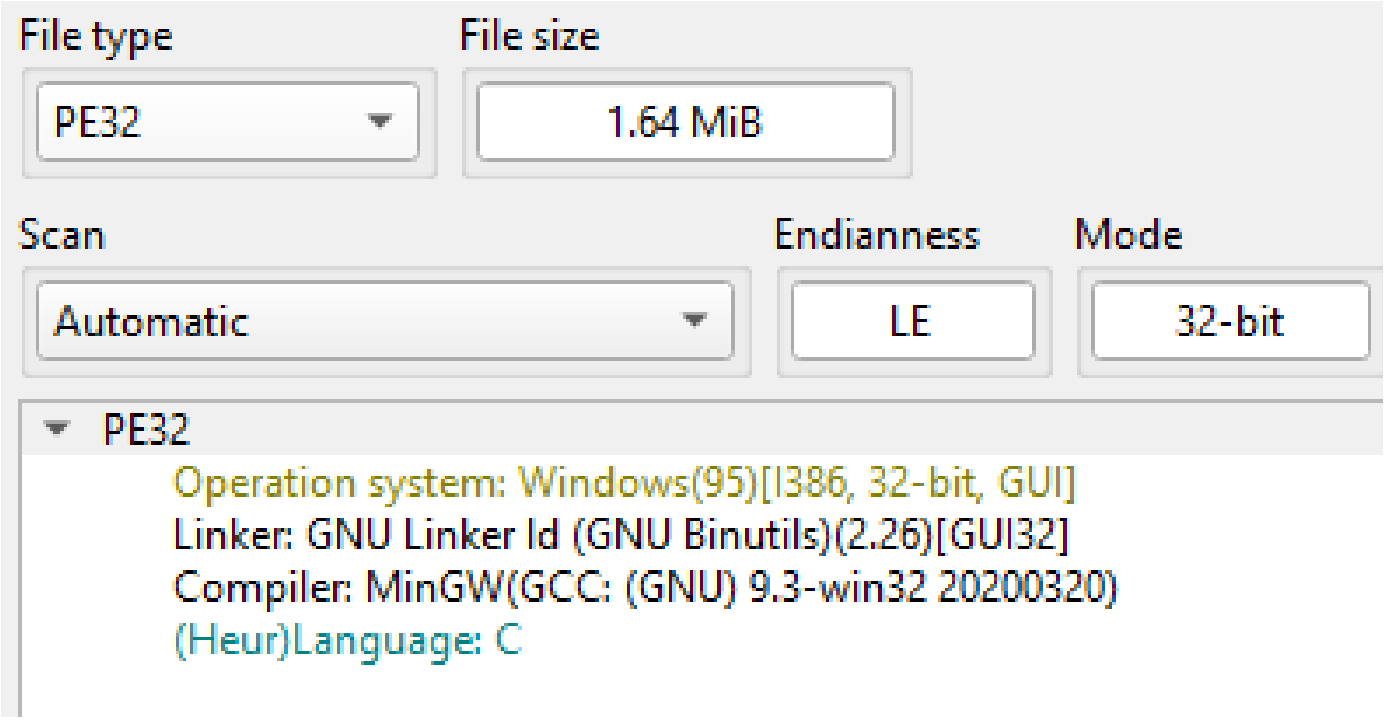
After the initial compromise, Scattered Spider deploys remote monitoring and management (RMM) tools or tunneling services to establish persistence. The group has been seen using ScreenConnect, AnyDesk, TeamViewer, Splashtop and similar utilities. Once inside the environment, Scattered Spider conducts extensive discovery, focusing on SharePoint, credential stores, VMware vCenter infrastructure, backup systems and documentation related to VPN setup and access. The group also enumerates Active Directory (AD) to map the network.

Recently, Scattered Spider has been using AWS Systems Manager Inventory to identify additional targets for lateral movement. They use extract, transform and load (ETL) tools to aggregate collected data into a centralized repository, which is then exfiltrated to attacker-controlled MEGA or Amazon S3 storage. Finally, Scattered Spider deploys the DragonForce ransomware payload and encrypts files across Windows, Linux, and ESXi systems.

## It's not a bug; it's a feature

During September, we spotted some fresh samples of DragonForce ransomware. Noticeably, these binaries were significantly larger than earlier variants. That seems to be due to a change in the developer's toolchain, as these samples are built using MinGW. While DragonForce is known to provide different ransomware strains to their

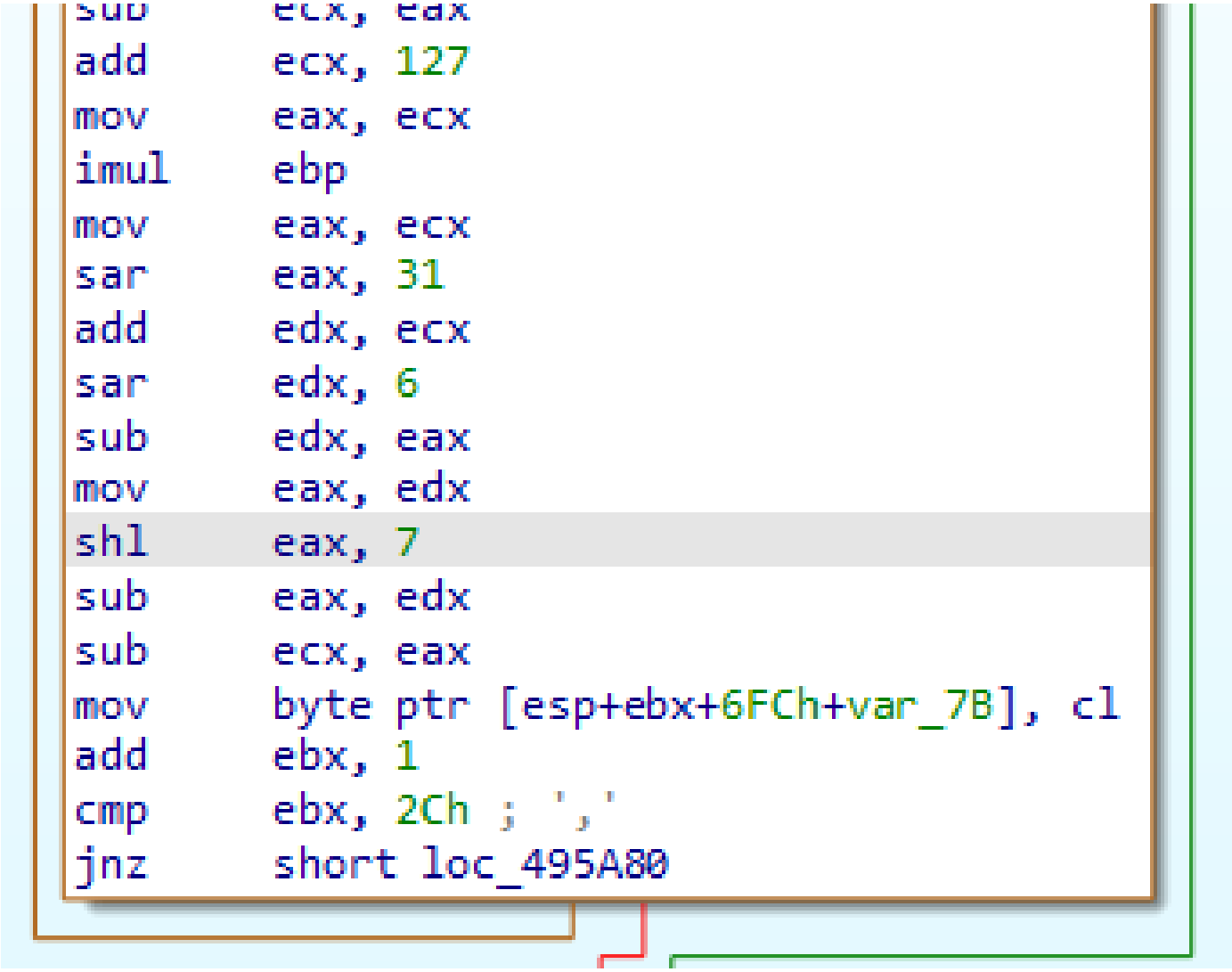
affiliates, this could also be a move to unify their development environment and provide a single ransomware strain for different platforms using the same codebase.




MinGW and the consolidation of DragonForce's codebase

Migrating code to new development environments often brings new bugs. In these samples, that come from Conti's codebase, we saw that the strings that are supposed to be encrypted using ADVObfuscator appear in clear text within the binary. That doesn't look like an intended update, as at runtime, the strings are encrypted and decrypted again before the program uses them.

Clear text strings within the binary that get encrypted and then decrypted at runtime




ADVObfuscator decryption loop

As expected, the analyzed code shows extensive overlap with Conti's leaked source files. It begins by invoking Conti's InitializeApiModule and DisableHooks functions, which set up the environment for ransomware execution and remove potential hooks within the Windows API.

DragonForce initialization process calling functions leveraged straight from Conti

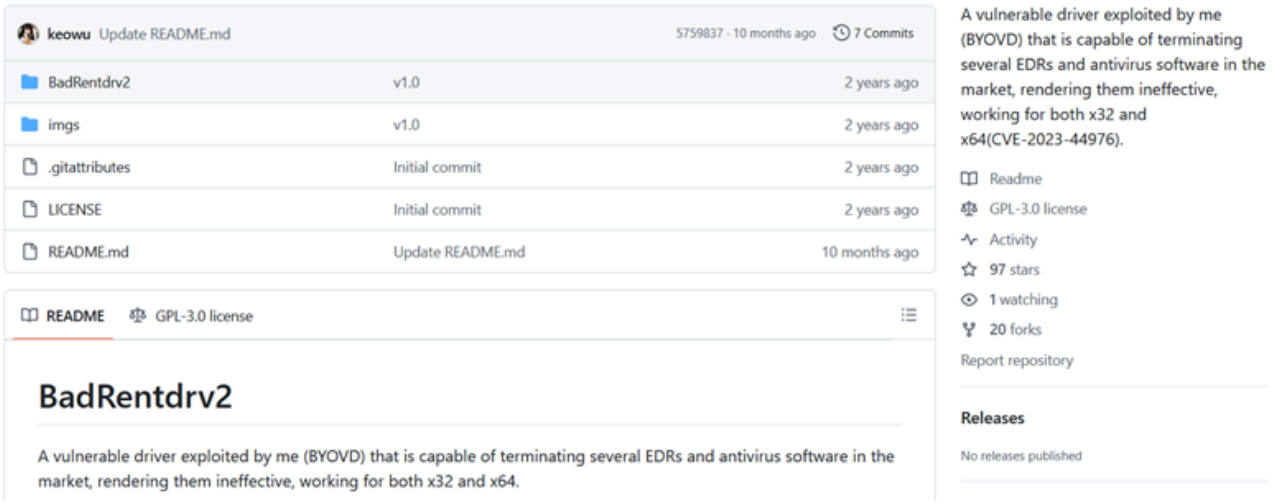
Next, DragonForce continues by decrypting and parsing its configuration, which consists of a binary file that is encrypted with the ChaCha20 algorithm. This configuration reflects the different customization options that the DragonForce builder provides to affiliates.

As is usually the case with ransomware, the builder allows configuring of custom encrypted file extensions, a list of file extensions to avoid and a list of software that could interfere with the encryption process to be terminated. This is an example of a parsed configuration:

- *custom_icon: 0*
- *custom_wallpaper: 0*
- *custom_extension: df_win*

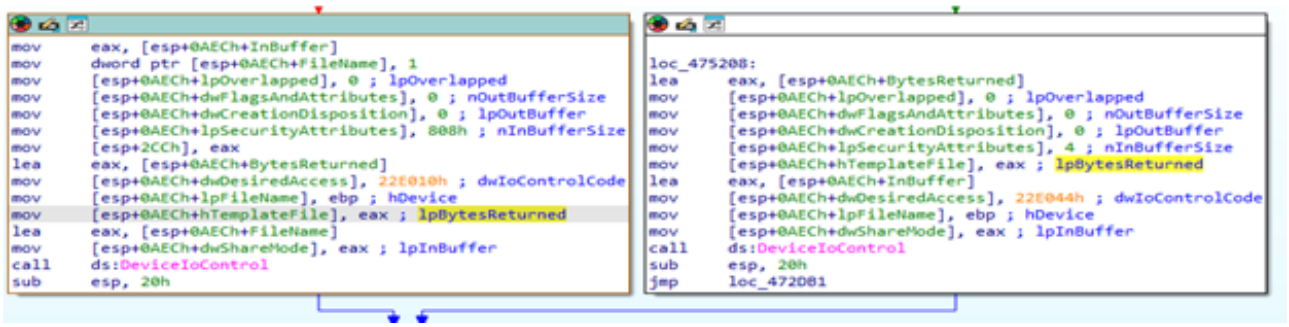
- *tyme_sync: 0*
- *encrypt_mode: 10*
- *full_encrypt_treshold: 2097152*
- *header_encrypt_treshold: 10485760*
- *header_encrypted_size: 3145728*
- *other_encrypt_chunk_percent: 10*
- *encrypt_file_names: 1*
- *schedule_job: 0*
- *kill: 1*
- *use_sys: 0*
- *priority: MsMpEng.exe, sql.exe, oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe, agntsvc.exe, isqlplussvc.exe, xfssvccon.exe, mysdesktopservice.exe, ocautopds.exe, encsvc.exe, firefox.exe, tbirdconfig.exe, mydesktopqos.exe, ocomm.exe, dbeng50.exe, sqbcoreservice.exe, excel.exe, infopath.exe, msaccess.exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe, steam.exe, thebat.exe, thunderbird.exe, visio.exe, winword.exe, wordpad.exe, notepad.exe, calc.exe, wuauclt.exe, onedrive.exe, SQLAGENT.exe, sqlserver.exe, SQLWrite.exe*
- *whitelist: 1*
- *path: tmp, winnit, temp, thumb, $Recycle.Bin, $RECYCLE.BIN, System Volume Information, Boot, Windows, perflogs, Public*
- *ext: .exe, .dll, .lnk, .sys, .msi, .bat, .DragonForce_encrypted*
- *filename: readme.txt*

The use_sysfield is particularly interesting. When enabled, instead of relying on normal process termination methods, the ransomware tries to abuse vulnerable kernel drivers (BYOVD) to stop processes. DragonForce supports two driver backends that must be present on the victim host beforehand: Truesight and BadRentdrv2.




A vulnerable driver that, when exploited (BYOVD), tries to terminate several EDRs and antivirus software in the market

By sending the proper control codes to those drivers through DeviceIoControl, operators can cause the drivers to terminate specified processes.

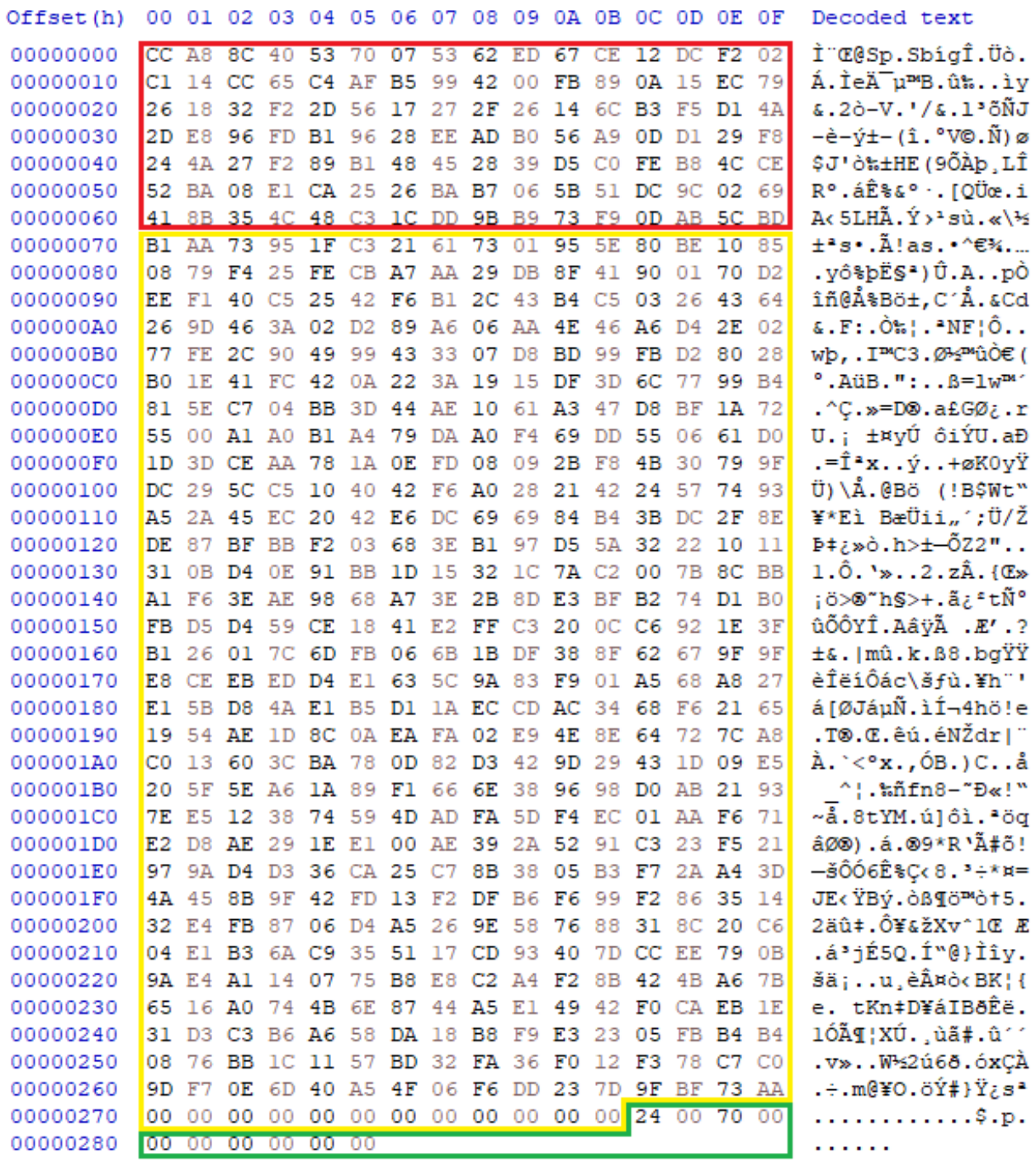



Known control codes that cause vulnerable rentdrv2 (left) and truesight (right) drivers to forcibly terminate other processes

The rest of the code is like Conti's base. As its predecessor, DragonForce will not only enumerate and encrypt local filesystems, but will also scan the local network looking for shared resources through SMB.

The encryption scheme remains the same, with a single ChaCha20 encryption key generated for each file, that is then encrypted using a public RSA key and appended at the beginning of the resulting file. At the end of it, a 10-byte blob of information on the encryption process is appended.

| Offset | Data |
| --- | --- |
| 0 | Encryption mode:<br>• Full = 0x24<br>• Partly = 0x25<br>• Header = 0x26 |
| 1 | Encryption percent:<br>• 0 = 100<br>• Any value from 1 to 99 |
| 2 | Encrypted data size |
| 3-9 | 0 |



| Offset(h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | Decoded text |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000 | CC | A8 | 8C | 40 | 53 | 70 | 07 | 53 | 62 | ED | 67 | CE | 12 | DC | F2 | 02 | Ì¨Œ@Sp.SbígÎ.Üò. |
| 00000010 | C1 | 14 | CC | 65 | C4 | AF | B5 | 99 | 42 | 00 | FB | 89 | 0A | 15 | EC | 79 | Á.ÌeÄ¯µ™B.û‰..ìy |
| 00000020 | 26 | 18 | 32 | F2 | 2D | 56 | 17 | 27 | 2F | 26 | 14 | 6C | B3 | F5 | D1 | 4A | &.2ò-V.'/&.l³õÑJ |
| 00000030 | 2D | E8 | 96 | FD | B1 | 96 | 28 | EE | AD | B0 | 56 | A9 | 0D | D1 | 29 | F8 | -è-ý±-(î.°V©.Ñ)ø |
| 00000040 | 24 | 4A | 27 | F2 | 89 | B1 | 48 | 45 | 28 | 39 | D5 | C0 | FE | B8 | 4C | CE | $J'ò‰±HE(9ÕÀþ¸LÎ |
| 00000050 | 52 | BA | 08 | E1 | CA | 25 | 26 | BA | B7 | 06 | 5B | 51 | DC | 9C | 02 | 69 | Rº.áÊ%&º·.[QÜœ.i |
| 00000060 | 41 | 8B | 35 | 4C | 48 | C3 | 1C | DD | 9B | B9 | 73 | F9 | 0D | AB | 5C | BD | A‹5LHÃ.Ý›¹sù.«\½ |
| 00000070 | B1 | AA | 73 | 95 | 1F | C3 | 21 | 61 | 73 | 01 | 95 | 5E | 80 | BE | 10 | 85 | ±ªs•.Ã!as.•^€¾.… |
| 00000080 | 08 | 79 | F4 | 25 | FE | CB | A7 | AA | 29 | DB | 8F | 41 | 90 | 01 | 70 | D2 | .yô%þË§ª)Û.A..pÒ |
| 00000090 | EE | F1 | 40 | C5 | 25 | 42 | F6 | B1 | 2C | 43 | B4 | C5 | 03 | 26 | 43 | 64 | îñ@Å%Bö±,C´Å.&Cd |
| 000000A0 | 26 | 9D | 46 | 3A | 02 | D2 | 89 | A6 | 06 | AA | 4E | 46 | A6 | D4 | 2E | 02 | &.F:.Ò‰¦.ªNF¦Ô.. |
| 000000B0 | 77 | FE | 2C | 90 | 49 | 99 | 43 | 33 | 07 | D8 | BD | 99 | FB | D2 | 80 | 28 | wþ,.I™C3.Ø½™ûÒ€( |
| 000000C0 | B0 | 1E | 41 | FC | 42 | 0A | 22 | 3A | 19 | 15 | DF | 3D | 6C | 77 | 99 | B4 | °.AüB.":..ß=lw™´ |
| 000000D0 | 81 | 5E | C7 | 04 | BB | 3D | 44 | AE | 10 | 61 | A3 | 47 | D8 | BF | 1A | 72 | .^Ç.»=D®.a£GØ¿.r |
| 000000E0 | 55 | 00 | A1 | A0 | B1 | A4 | 79 | DA | A0 | F4 | 69 | DD | 55 | 06 | 61 | D0 | U.¡ ±¤yÚ ôiÝU.aÐ |
| 000000F0 | 1D | 3D | CE | AA | 78 | 1A | 0E | FD | 08 | 09 | 2B | F8 | 4B | 30 | 79 | 9F | .=Îªx..ý..+øK0yŸ |
| 00000100 | DC | 29 | 5C | C5 | 10 | 40 | 42 | F6 | A0 | 28 | 21 | 42 | 24 | 57 | 74 | 93 | Ü)\Å.@Bö (!B$Wt" |
| 00000110 | A5 | 2A | 45 | EC | 20 | 42 | E6 | DC | 69 | 69 | 84 | B4 | 3B | DC | 2F | 8E | ¥*Eì BæÜii„´;Ü/Ž |
| 00000120 | DE | 87 | BF | BB | F2 | 03 | 68 | 3E | B1 | 97 | D5 | 5A | 32 | 22 | 10 | 11 | Þ‡¿»ò.h>±—ÕZ2".. |
| 00000130 | 31 | 0B | D4 | 0E | 91 | BB | 1D | 15 | 32 | 1C | 7A | C2 | 00 | 7B | 8C | BB | 1.Ô.'»..2.zÂ.{Œ» |
| 00000140 | A1 | F6 | 3E | AE | 98 | 68 | A7 | 3E | 2B | 8D | E3 | BF | B2 | 74 | D1 | B0 | ¡ö>®˜h§>+.ã¿²tÑ° |
| 00000150 | FB | D5 | D4 | 59 | CE | 18 | 41 | E2 | FF | C3 | 20 | 0C | C6 | 92 | 1E | 3F | ûÕÔYÎ.AâÿÃ .Æ'.? |
| 00000160 | B1 | 26 | 01 | 7C | 6D | FB | 06 | 6B | 1B | DF | 38 | 8F | 62 | 67 | 9F | 9F | ±&.\|mû.k.ß8.bgŸŸ |
| 00000170 | E8 | CE | EB | ED | D4 | E1 | 63 | 5C | 9A | 83 | F9 | 01 | A5 | 68 | A8 | 27 | èÎëíÔác\šƒù.¥h¨' |
| 00000180 | E1 | 5B | D8 | 4A | E1 | B5 | D1 | 1A | EC | CD | AC | 34 | 68 | F6 | 21 | 65 | á[ØJáµÑ.ìÍ¬4hö!e |
| 00000190 | 19 | 54 | AE | 1D | 8C | 0A | EA | FA | 02 | E9 | 4E | 8E | 64 | 72 | 7C | A8 | .T®.Œ.êú.éNŽdr\|¨ |
| 000001A0 | C0 | 13 | 60 | 3C | BA | 78 | 0D | 82 | D3 | 42 | 9D | 29 | 43 | 1D | 09 | E5 | À.`<ºx.‚ÓB.)C..å |
| 000001B0 | 20 | 5F | 5E | A6 | 1A | 89 | F1 | 66 | 6E | 38 | 96 | 98 | D0 | AB | 21 | 93 | _^¦.‰ñfn8–˜Ð«!" |
| 000001C0 | 7E | E5 | 12 | 38 | 74 | 59 | 4D | AD | FA | 5D | F4 | EC | 01 | AA | F6 | 71 | ~å.8tYM.ú]ôì.ªöq |
| 000001D0 | E2 | D8 | AE | 29 | 1E | E1 | 00 | AE | 39 | 2A | 52 | 91 | C3 | 23 | F5 | 21 | âØ®).á.®9*R'Ã#õ! |
| 000001E0 | 97 | 9A | D4 | D3 | 36 | CA | 25 | C7 | 8B | 38 | 05 | B3 | F7 | 2A | A4 | 3D | —šÔÓ6Ê%Ç‹8.³÷*¤= |
| 000001F0 | 4A | 45 | 8B | 9F | 42 | FD | 13 | F2 | DF | B6 | F6 | 99 | F2 | 86 | 35 | 14 | JE‹ŸBý.òß¶ö™ò†5. |
| 00000200 | 32 | E4 | FB | 87 | 06 | D4 | A5 | 26 | 9E | 58 | 76 | 88 | 31 | 8C | 20 | C6 | 2äû‡.Ô¥&žXvˆ1Œ Æ |
| 00000210 | 04 | E1 | B3 | 6A | C9 | 35 | 51 | 17 | CD | 93 | 40 | 7D | CC | EE | 79 | 0B | .á³jÉ5Q.Í"@}Ìîy. |
| 00000220 | 9A | E4 | A1 | 14 | 07 | 75 | B8 | E8 | C2 | A4 | F2 | 8B | 42 | 4B | A6 | 7B | šä¡..u¸èÂ¤ò‹BK¦{ |
| 00000230 | 65 | 16 | A0 | 74 | 4B | 6E | 87 | 44 | A5 | E1 | 49 | 42 | F0 | CA | EB | 1E | e. tKn‡D¥áIBðÊë. |
| 00000240 | 31 | D3 | C3 | B6 | A6 | 58 | DA | 18 | B8 | F9 | E3 | 23 | 05 | FB | B4 | B4 | 1ÓÃ¶¦XÚ.¸ùã#.û´´ |
| 00000250 | 08 | 76 | BB | 1C | 11 | 57 | BD | 32 | FA | 36 | F0 | 12 | F3 | 78 | C7 | C0 | .v»..W½2ú6ð.óxÇÀ |
| 00000260 | 9D | F7 | 0E | 6D | 40 | A5 | 4F | 06 | F6 | DD | 23 | 7D | 9F | BF | 73 | AA | .÷.m@¥O.öÝ#}Ÿ¿sª |
| 00000270 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 24 | 00 | 70 | 00 | ............$.p. |
| 00000280 | 00 | 00 | 00 | 00 | 00 | 00 | | | | | | | | | | | ...... |

Encrypted file structure, where the red block – encrypted data, the yellow block – encrypted ChaCha20, and the green block – encryption information

In the different ransom notes dropped by recent samples, operators threaten their victims to delete the decryptor and make their data public by the 2nd and 22nd of September, proving that the DragonForce platform is still being used to conduct ransomware attacks.

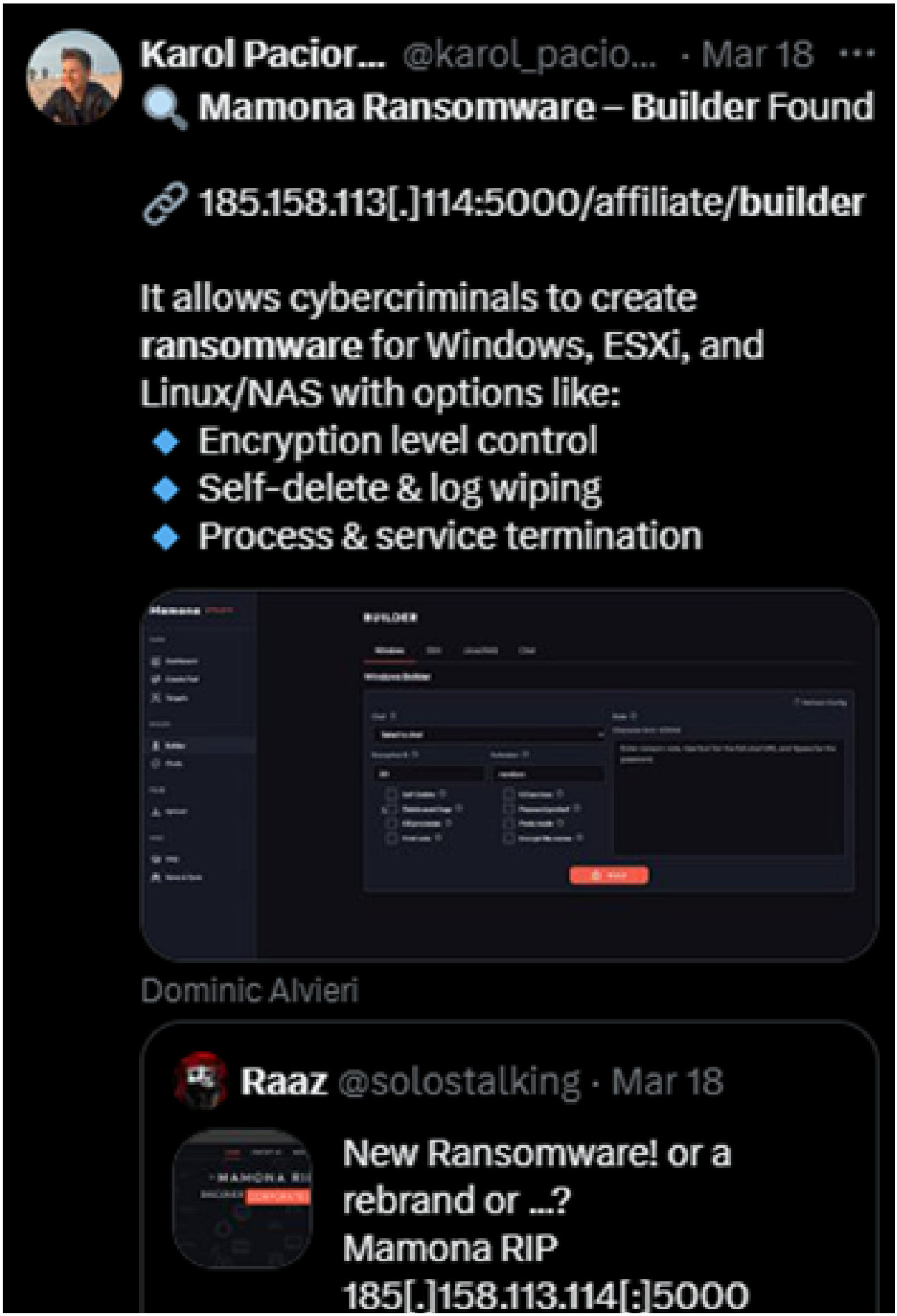
## DragonForce affiliates and the Devman connection

One of the clearest indications of DragonForce's growing presence in the ransomware landscape lies in its growing number of affiliates, particularly those moving from one ransomware group to another. Recently, we have found samples of Devman ransomware built using DragonForce's builder. This sample has '.devman' as the encrypted file extension in its configuration, but other functionalities like the icon, wallpaper, and ransom note are all from DragonForce.

The connection between DragonForce and Devman can also be seen in the similarities of their ransom note structure. Devman, which initially began deploying a Mamona-based variant around May 2025, used a ransom note format that closely mirrors DragonForce's LockBit-based variant which was first seen in the wild around mid-2023. This resemblance may not be a coincidence. The time gap between both samples and the builder used on both samples suggests that Devman may have been an early DragonForce affiliate experimenting to create its own branding while continuing to rely on DragonForce's infrastructure and tools.


Comparison of DragonForce (top) and Devman (bottom) ransom notes showing similar formatting and content

Digging deeper into Devman, its choice of using Mamona ransomware builder revealed more details about its affiliations. Mamona ransomware is first introduced in March 2025 by the underground forum user known as “$$”, the same operator behind Eldorado and Blacklock ransomware. While Mamona quickly lost traction, it was soon rebranded as Global ransomware, though still under the control of the same operator.


Karol Pacior... @karol_pacio... · Mar 18
Mamona Ransomware – Builder Found
185.158.113[.]114:5000/affiliate/builder
It allows cybercriminals to create ransomware for Windows, ESXi, and Linux/NAS with options like:
Encryption level control
Self-delete & log wiping
Process & service termination
Dominic Alvieri
Raaz @solostalking · Mar 18
New Ransomware! or a rebrand or ...?
Mamona RIP
185[.]158.113.114[:]5000


An external researcher on X posted about the Mamona ransomware builder being hosted at: 185.158.113[.]114:5000/affiliate/builder. The /affiliate/builder path suggests that the builder is only accessible to affiliates. This detail highlights the connection between Devman being an affiliate of Mamona.

Furthermore, Devman having both Mamona and DragonForce encryptors in its arsenal aligns with the cartel-like structure that DragonForce is trying to promote where its affiliates can create their own brand while operating within the DragonForce cartel ecosystem.

Beyond ransomware groups, DragonForce has also expanded its partnerships to include other cybercriminal groups within the broader underground ecosystem. Scattered Spider is one that they had partnered with after branding themselves as a "cartel." Scattered Spider is known for partnering with other notorious RaaS operators in the past, such as BlackCat, RansomHub, and Qilin, providing initial access to the victim's network and handing over the access for ransomware deployment. This recent partnership drew significant attention after the attack on major U.K. retailer Marks & Spencer, which researchers attribute to Scattered Spider–DragonForce operations. Though not confirmed, this incident fits the timeline of DragonForce's rebrand just a month before, showing that Scattered Spider was quick to leverage DragonForce in its operations.

## Power struggles among ransomware cartels

By rebranding itself as a "cartel," DragonForce aimed to strengthen its influence and alliances in the ransomware landscape, proving its dominance by defacing or taking control of rival groups' infrastructure. Its earliest move was the defacement of BlackLock's leak site.


Dominic Alvieri @AlvieriD · Mar 19
Am I'm seeing things...did DragonForce just hack BlackLock because this looks posted on the BlackLock leak site.
It is not good...
DragonForce
DragonForce – work without paranoia
/etc/passwd
.env (Oh-no...)
Chat dump
It is not good...
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
tss:x:59:59:Account used for TPM access:/:/sbin/nologin
polkitd:x:998:998:User for polkitd:/:/sbin/nologin
clevis:x:997:993:Clevis Decryption Framework unprivileged
user:/var/cache/clevis:/sbin/nologin
unbound:x:996:992:Unbound DNS resolver:/etc/unbound:/sbin/nologin
libstoragemgmt:x:995:991:daemon account for
libstoragemgmt:/var/run/lsm:/sbin/nologin
dnsmasq:x:990:990:Dnsmasq DHCP and DNS
server:/var/lib/dnsmasq:/sbin/nologin
cockpit-ws:x:989:989:User for cockpit web
service:/nonexisting:/sbin/nologin

Report on X about BlackLock's leak site defacement

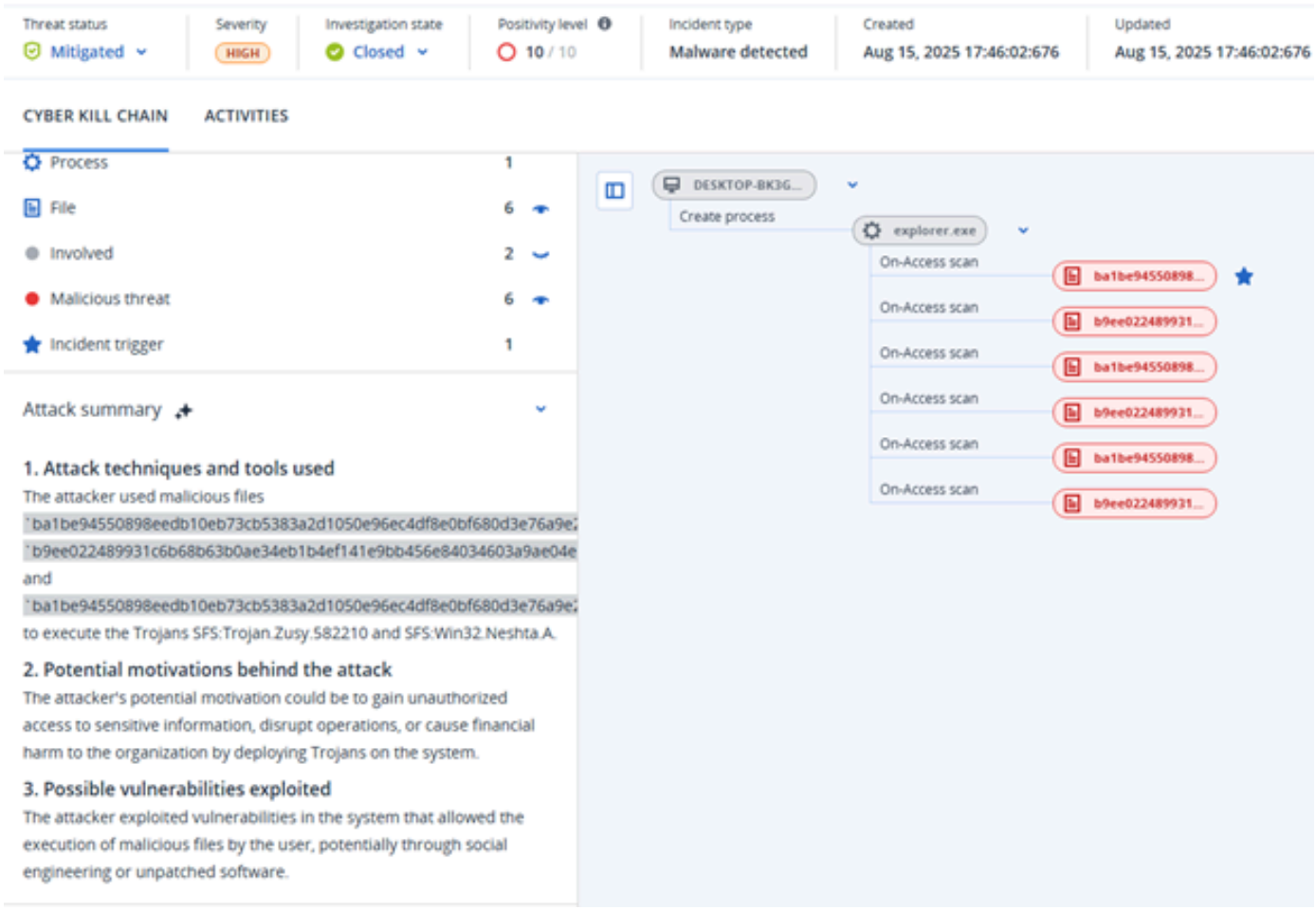
A few weeks after this first incident, DragonForce attempted a "hostile takeover" on RansomHub's infrastructure. This allegedly caused RansomHub to stop its operations, with its affiliates fleeing to rival groups like Qilin and DragonForce.

## Conclusion

Similar to ransomware such as Akira, Royal and Black Basta, DragonForce used the Conti leaked source code to forge a dark successor crafted to carry its own mark. While other groups made some changes to the code to give it a different spin, DragonForce kept all functionality unchanged, only adding an encrypted configuration in the executable to get rid of command-line arguments that were used in the original Conti code.

By fixing Akira's encryption flaws and strengthening its cipher, this threat actor has focused on steadily expanding its victim list and recruiting new affiliates, proving itself as a significant and persistent threat.

## Detected by Acronis



Report on X about BlackLock's leak site defacement

# Indicators of Compromise

### Portable executable (PE)

4db090498a57b85411417160747ffd8d4875f98b3ca2b83736a68900b7304d2b
f58af71e542c67fbacf7acc53a43243a5301d115eb41e26e4d5932d8555510d0

e4c44d0f462fce02b2c31555b12c022cdd6eae6492fd3a122e32e105fc5a54f8

f5df98b344242c5eaad1fce421c640fadd71f7f21379d2bf7309001dfeb25972
44994c720ad936809b54388d75945abd18b5707e20c9ee8f87b8f958ca8f5b16

0dfe23ab86cb5c1bfaf019521f3163aa5315a9ca3bb67d7d34eb51472c412b22

56dfe55b016c08f09dd5a2ab58504b377a3cd66ffba236a5a0539f6e2e39aa71

ad158a9ef5e849f7a2d10828a9aed89ebded7a2b5b3abb765f5797051cdf4a20

451a42db9c514514ab71218033967554507b59a60ee1fc3d88cbeb39eec99f20

dca4102fba483bf0060427e0d583a1f61d079bf0754db4d61ff2969cc1bc3474

df5ab9015833023a03f92a797e20196672c1d6525501a9f9a94a45b0904c7403

80e3a04fa68be799b3c91737e1918f8394b250603a231a251524244e4d7f77d9

d67a475f72ca65fd1ac5fd3be2f1cce2db78ba074f54dc4c4738d374d0eb19c7

1ccf8baf11427fae273ffed587b41c857fa2d8f3d3c6c0ddaa1fe4835f665eba

b10129c175c007148dd4f5aff4d7fb61eb3e4b0ed4897fea6b33e90555f2b845

c844d02c91d5e6dc293de80085ad2f69b5c44bc46ec9fdaa4e3efbda062c871c

b9bba02d18bacc4bc8d9e4f70657d381568075590cc9d0e7590327d854224b32

**ELF**

8e8f463c37ea7133194731bfe4490e6713dd0133f30fe08a6d069d10fa7db2c6

941b0bb479946c833a0436ecb84b94c8468c86c40016f46029e8bf04a22a754e

**Ransom notes**

**1 - 04b14ead49adea9431147c145a89c07fea2c6f1cb515d9d38906c7696d9c91d5**

*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 02/09/2025 00:00 UTC.*

*- # 1 Communication Process,*

*In order to contact us you need to click on the special link below, which is listed in #2.*

*After that the negotiation process begins, in which you have the opportunity to request several things from us,*

*1. Make a test decrypt.*

*2. Get a list of the files stolen from you.*

*At the conclusion of our negotiations we agree on a price, we set the price ourselves based on your income/your insurance.*

*We scrutinize your documents and are well aware of how much income your company has per year.*

*- # 2 Access to the meeting room,*

*To access us please download Tor Browser which is available here. (https://www.torproject.org/)*

*Once you download the special anonymous browser you need to follow this link,*
*http://3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd.onion*

*Your unique ID: F744871F84DDF60CF744871F84DDF60C - use it to enter our meeting room.*

*- # 3 Additional Support Contacts,*

*Tox: 1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20*

*- # 4 Recommendations,*

*Do not try to recover your files with third-party programs, you will only do harm.*

*Do not turn off / reboot your computer.*

*Be courteous in our meeting room.*

*Do not procrastinate.*

*- # 5 Blog and News,*

*Blog: http://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion*

*DragonNews: http://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion/news*

***2 - 849ef3cf2c251f6088d735c7b67c3434e915a1d924efecf4d608dbe9bb01928a***

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 22/09/2025 00:00 UTC.

- # 1 Communication Process,

In order to contact us you need to click on the special link below, which is listed in #2.

After that the negotiation process begins, in which you have the opportunity to request several things from us,

1. make a test decrypt.

2. get a list of the files stolen from you.

At the conclusion of our negotiations we agree on a price, we set the price ourselves based on your income/your insurance.

We scrutinize your documents and are well aware of how much income your company has per year.

- # 2 Access to the meeting room,

To access us please download Tor Browser which is available here. (https://www.torproject.org/)

Once you download the special anonymous browser you need to follow this link,
http://3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd.onion

Your unique ID: F73EB3EEF76498F4F73EB3EEF76498F4 - use it to enter our meeting room.

- # 3 Additional Support Contacts,

Tox: 1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20

- # 4 Recommendations,

Do not try to recover your files with third-party programs, you will only do harm.

Do not turn off / reboot your computer.

Be courteous in our meeting room.

Do not procrastinate.

- # 5 Blog and News,

Blog: http://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion

DragonNews: http://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion/news