DragonForce Ransomware: Unveiling Its Tactics and Impact

Idan Malihi

Security Researcher

Written by Idan Malihi and Yaniv Azran

Key Findings

- DragonForce has transformed from a politically motivated cyber group into a financially driven ransomware operation. Originally associated with pro-Palestinian cyber activities, the group has broadened its focus beyond hacktivism to include ransomware, data leaks, and financial extortion in its strategy. Their current operations target Israeli entities as well as global organizations.
- The group employs a structured extortion model that utilizes a maintained Dark Web leak site. They publicly display victim data, ransom negotiations, and countdown timers, which creates a fear-driven incentive for the victims to pay. Their infrastructure includes Tor-based communication channels, encrypted messaging (using Tox), and automated ransom-tracking systems.
- DragonForce Ransomware is based on the LockBit builder from 2022, utilizing similar configurations and attack methods. The ransomware's icon and wallpaper are embedded in the binary's overlay, compressed with Zlib, and loaded dynamically during execution. This technique enables stealthy deployment and helps evade static detection, supporting the idea that DragonForce has repurposed the leaked tools from LockBit for its own operations.
- DragonForce employs double extortion tactics to exert maximum pressure on its victims. The ransom note is carefully structured, threatening both the encryption of data and public exposure, stating that stolen files will be leaked if the ransom is not paid. Additionally, the malware's automated extortion framework enhances its effectiveness in high-profile attacks, positioning DragonForce as a significant ransomware threat in 2025.

Evolution of Cyber Threat Groups

In recent years, there has been a notable increase in cyberattacks around the globe. Organized threat groups, often motivated by political ideologies or financial gain, have intensified their activities, targeting critical infrastructure, government institutions, and private organizations.

Most of these attacks follow a systematic and organized approach, which typically includes:

- Initial compromise – Gaining unauthorized access to the target network.
- Data exfiltration – Stealing sensitive information before encryption.
- Encryption of files – Locking access to critical data and systems.
- Extortion and ransom demands – Threatening to leak stolen data unless payment is made.

Over time, threat actors have refined their attack methods, investing in advanced infrastructure to manage data leaks, ransom negotiations, and operational security. Many groups create dedicated dark web leak sites where they publish details about their victims, share samples of data breaches, and even disclose ransom negotiations, which further pressures organizations to meet their demands.

In the ever-changing landscape of cybersecurity, DragonForce has become a prominent cyber threat group known for its well-organized attack and leak mechanisms. Unlike traditional ransomware groups that primarily seek financial gain, DragonForce employs a combination of ideological tactics and extortion strategies. A key weapon in their arsenal is the extensive public exposure they create on darknet platforms, targeting organizations effectively. The group’s coordinated approach to disrupting businesses through cyber warfare and financial extortion positions it as a significant player in the realm of modern cyber threats.

Introduction – DragonForce

DragonForce is a Malaysia-based cyber threat group that has quickly gained notoriety in the cybercrime landscape due to its high-profile cyberattacks, particularly targeting entities in Israel and other global organizations. The group primarily operates from ideological motives, aligning itself with pro-Palestinian causes and using cyber warfare as a means of activism and disruption.

In addition to its cyber operations, DragonForce has been actively involved in propaganda and psychological warfare. DragonForce effectively uses social media, forums, and darknet communities to amplify its message and attract new members.

DragonForce is not only focused on politically motivated cyberattacks. Over time, the group has expanded its operations to include financially driven cybercrime, particularly through ransomware and data extortion campaigns. They have been linked to attacks targeting businesses, where they demand ransom payments and threaten to leak stolen data on dark web forums. This shift illustrates how DragonForce has evolved from a hacktivist collective into an organized cybercriminal entity, combining ideological goals with financial incentives.

DragonForce’s Cyber Activities Against Israel

In June 2021, after Israel announced its intention to establish diplomatic relations with Southeast Asian Muslim countries, the group DragonForce launched a coordinated wave of cyberattacks against Israeli targets. This marked a significant escalation in the group’s operations, showcasing its capabilities and willingness to engage in politically motivated cyber warfare (https://therecord.media/new-dragonforce-hacktivist-group-causes-havoc-in-israel)

One of the most notable attacks attributed to DragonForce during this period targeted Israel’s banking infrastructure, leading to temporary service disruptions. This attack highlighted the group’s technical skills and strategic objectives, establishing DragonForce as a capable and ideologically driven threat actor.

This campaign represented a defining moment for DragonForce, solidifying its status as an emerging hacktivist entity that employs both disruptive tactics and financially motivated attack strategies. Over time, the group has refined its techniques and expanded its focus from politically charged cyber-attacks to include broader ransomware and extortion-based operations.

The group's attacks are primarily politically motivated; however, some of its activities extend across various industries and regions. It has claimed responsibility for a wide range of attacks, including DDoS attacks and data breaches.

DragonForce's Leak Site and Propaganda Strategy

DragonForce runs a well-organized and systematically maintained leak site on the dark web, serving as a centralized platform for exposing compromised organizations. Each breached company has its own dedicated page, which includes a brief description of the business and, in some cases, additional identifiable details.

A key feature of the site is a countdown timer set to 14 days from the moment the breach is disclosed. This deadline mechanism is designed to create psychological pressure on the victims, pushing them to comply with ransom demands. If the affected company fails to pay within the specified timeframe, DragonForce publicly releases the stolen data along with chat logs of their negotiations with the victim.

A notable example from this research highlighted a negotiation attempt between a victim company and DragonForce. The company sought to reduce the ransom amount, but the group refused to make any concessions. They emphasized the urgency of the countdown timer and warned that failure to pay would lead to the full disclosure of the stolen data. By making these negotiations public, DragonForce sends a clear message to future victims: negotiations are futile, and the only way to prevent exposure is to pay the ransom in full.

Once the countdown expires, the stolen files become publicly accessible directly from the site. The files are neatly categorized, allowing anyone to browse through the leaked documents without needing to download them. The exposed data often includes financial records, employee and customer information, internal communications, contracts, and other highly sensitive documents. This structured data exposure model adds pressure, reinforcing DragonForce’s ultimatum: **comply or face full-scale data disclosure**.

In addition to its dark web infrastructure, DragonForce actively operates a Telegram channel that serves as an alternative platform for propaganda and information dissemination. This channel is used for the following purposes:

- Announcing successful attacks
- Publishing ideological statements
- Sharing recruitment materials

One notable example uncovered during this research reveals DragonForce bragging about a successful breach of an Israeli server. This post included a command output that verified the compromised IP address and its association with an Israeli network. The messaging also contained propaganda aimed at reinforcing the group's ideological stance while subtly suggesting potential future attacks. To enhance its impact, the post included a link to Zone-H, a well-known defacement archive website, which further publicized the breach and maximized its visibility.

DragonForce has emerged as one of the most prominent cyber threat groups in recent years. They effectively combine advanced cyberattacks, public extortion, and aggressive propaganda campaigns on both dark web platforms and Telegram. By publicizing the names of their victims, leaking confidential negotiations, exposing highly sensitive data, and creating ideological content, the group applies sustained pressure on its targets while also strengthening its presence in the global cyber warfare landscape.

Having analyzed DragonForce’s threat intelligence profile and attack methodologies, the next section will present a detailed technical examination of the malware samples used in their operations.

Dissecting the Threat: DragonForce Ransomware

Technical Details

File Name: DragonForce.exe
File Type: Portable Executable
Architecture: PE32 (32-bit)
Size: 418KB
MD5: 05f1a39c0902297debceb4c9c4c6674c
SHA256: 70afd8efb34382badead93ae104d958256de6be8054227ccc85fe95d5c5f9db0

Static Analysis

The ransomware is a 32-bit executable compiled using Microsoft Visual Studio, likely in the C++ programming language. Additionally, the file appears to be packed or compressed. According to DIE, the ransomware compresses some data using the Zlib module and decompresses this specific data during runtime in the offset of 0x66400 and the size of the data 0x2608 (9736 bytes).

The ransomware's entropy analysis suggests that only the overlay is packed. This indicates that the file itself is not actually packed; instead, it conceals some data within the binary inside the overlay. Essentially, this means that the compressed data is hidden at the end of the file (EOF).

I utilized `Binwalk` to analyze the binary ransomware and identify the various types of data concealed within it, thereby gaining insight into what files the attacker was attempting to hide from researchers and analysts. It contains an XML document that serves as the manifest file. Finally, there are two compressed files that the ransomware will utilize during its runtime.

To extract both compressed files, I executed a Python script that reads and extracts the data located at the `0x66400` and `0x66D24` offsets.

The compressed files are graphic files used in the ransomware's operations when it drops files related to the ransomware during runtime.

```
firstFile.ico: a0bbc666c39f80d6ac18ae1b253c3462
```

```
secondFile.png: 07fb997df804901c7f09bcce85ec2c05
```

In addition, the ransomware encrypts the victim’s files using the symmetric `ChaCha20` encryption method with a key of 256 bytes.

Compilation Time

The ransomware was compiled on Mon, 09/23/2024.

Strings

The malware utilizes the ASLR (Address Space Layout Randomization) mechanism to hinder debugging or reverse engineering efforts and randomizes the memory location where the ransomware is loaded.

The strings below indicate that ransomware utilizes the `ChaCha20` encryption method. These strings relate to the key expansion process in the `ChaCha20` stream cipher, which is typically used for fast and secure encryption.

The following strings indicate that the ransomware uses logs printed during runtime to determine the status of its operations, including file name changes, run path, privilege escalation, desktop wallpaper changes, and more.

The string `SELECT * FROM Win32_ShadowCopy` shows that the ransomware is using WMI to query Volume Shadow Copies, which disables the victim's ability to restore backups.

The following strings relate to the extensions that the threat actor configures for the ransomware, specifying which extensions to encrypt on the victim's system.

The ransomware appears to be conducting reconnaissance on network shares and facilitating lateral movement to locate and encrypt files stored on shared network drives.

Dissecting the DragonForce Ransomware

During the ransomware's initial execution, the ransomware uses dynamic API resolution to conceal malware characteristics and functionalities. It is called the `4011A0` subroutine, which is responsible for loading the relevant DLL files into its memory space using the `LoadLibraryA` function so it can perform its operations correctly.

The ransomware generates a log file named `log.log` located in the `C:\Users\Public` directory to track its operations.

The ransomware configures which file extensions it will not encrypt, such as .exe, .dll, .lnk, etc.

The `421570` subroutine is responsible for the encryption process configuration. It seems that the ransomware configures dynamic configurations for efficient encryption, process termination, and system disruption. The presence of keys such as `encrypt_mode`, `full_encrypt_threshold`, and `encrypt_file_names` suggests that the ransomware employs selective encryption techniques to optimize the speed of the encryption process. Additionally, strings like `custom_wallpaper` and `custom_extension` indicate that the malware modifies the desktop wallpaper and changes the files' extension. Furthermore, the ransomware targets several system and database processes to terminate them and encrypt them, such as:

Security and System Processes	Database Processes	User Applications
MsMpEng.exe	sql.exe	excel.exe
wuauclt.exe	SQLAGENT.exe	infopath.exe

	sqlservr.exe	msaccess.exe
	SQLWriter.exe	mspub.exe
	oracle.exe	onenote.exe
	dbsnmp.exe	outlook.exe
	agntsvc.exe	powerpnt.exe
	ocssd.exe	onedrive.exe
	isqlplussvc.exe	visio.exe
	dbeng50.exe	winword.exe
	sqbcoreservice.exe	wordpad.exe
		notepad.exe
		synctime.exe
		xfssvccon.exe
		mydesktopservice.exe
		ocautoupds.exe
		encsvc.exe
		tbirdconfig.exe
		mydesktopqos.exe
		ocomm.exe

	steam.exe
	thebat.exe
	thunderbird.exe
	calc.exe

At the end of the configurations, it writes to the `log.log` file.

In the following flow, the ransomware retrieves the current process ID using the `GetCurrentProcessId` function, which is then used in the `42A7A0` subroutine.

In the subroutine, the ransomware uses the `OpenProcess` function with the `0x400` parameter, which is related to the `PROCESS_QUERY_INFORMATION` access rights. This suggests an attempt to query the process's security context. If the function's execution is successful, it jumps to the `42A9E5` memory location, where it calls `OpenProcessToken` and `GetTokenInformation` to extract the security details about the running process.

Additionally, it calls `LookupAccountSidW` to resolve the account name associated with the SID (security identifier). The ransomware might determine whether it is executing under a privileged user. Then, it writes in the logs the privileges execution as a `“Running under: %s”` string.

The configuration of DragonForce Ransomware shows similarities to the LockBit builder that was leaked in 2022. Key settings observed include `encrypt_mode`, `local_disks`, `network_shares`, `kill_processes`, `kill_services`, `set_wallpaper`, and `set_icons`, all of which match the structure of LockBit's leaked `config.json`. This suggests that DragonForce may be a modified version of the original LockBit builder. Additionally, DragonForce incorporates several defense evasion techniques, including anti-forensics parameters like `kill_defender`, `delete_eventlogs`, and `self_destruct`. These features indicate that the ransomware aims to disable security defenses and eliminate forensic evidence. Furthermore, its functionality to alter desktop wallpaper and icons through `set_wallpaper` and `set_icons` is similar to the behavior of LockBit ransomware.

The malware checks and verifies whether the process has been executed with administrative privileges, which is crucial for the ransomware's subsequent operations. The ransomware is attempting to retrieve the security token to determine whether it has administrator or SYSTEM-level privileges. The sequence begins with a call to `GetCurrentProcess`, followed by `OpenProcessToken`, which allows access to the token of the current process. After obtaining the token, it is called `GetTokenInformation`, which is used to extract information about privilege levels, user group details, or integrity levels. The ransomware then evaluates the retrieved token information. If the token handle is valid, the execution continues; if not, the ransomware process terminates. Analysis of the ransomware's runtime value indicates it was executed with high privileges, as shown by the `“Process is elevated: %d”` value being `1`.

The ransomware creates a mutex during runtime using `CreateMutexA` to ensure that only a single instance runs, preventing reinfection.

```
Mutex: hsfjuukjzloqu28oajh727190
```

The ransomware scans the victim’s system for logical drives using `GetLogicalDriveStringsW`. This operation is crucial for the ransomware to identify which drives exist in the victim’s system and to infect them during execution.

After the ransomware configures the kill processes list, it looks for processes that are running on the victim's system and compares them to the list. It uses `OpenProcess` to access the `notepad.exe` process and then terminates it using `TerminateProcess`.

The ransomware employs the `NetShareEnum` function to facilitate lateral movement, expanding its encryption capabilities to network shares and NetBIOS. It configures the `servername` parameter to three types of subnets: `172.X.X.X`, `192.168.0.X`, and

169.X.X.X, which are commonly used subnets in organizations worldwide. The level parameter is set to 1, which, according to Microsoft’s documentation, indicates that it will return details about shared resources, including the resource name and type.

The ransomware then decompresses two files from its overlay and drops them into the `C:\Users\Public` folder: `icon.ico` and `wallpaper_white.png`.

It then begins the process of encrypting the victim’s files. For each file, the ransomware encrypts its contents, changes the file’s name, and modifies the extension using `MoveFileW`.

It then creates `readme.txt` files using the `CreateFileW` function in every directory whose content has been encrypted.

The DragonForce Ransomware ransom note utilizes psychological pressure and clear communication to coerce victims into paying the ransom. It outlines the impact of the attack, the communication process, payment instructions, and the consequences of non-compliance. The note is signed as: 01000100 `01110010 01100001 01100111 01101111 01101110 01000110 01101111 01110010 01100011 01100101` This is the binary representation of “DragonForce,” which confirms the ransomware strain responsible for the attack.

Conclusion

Our research indicates that DragonForce operates as a hacktivist group, blending hacktivism with financially motivated cyber extortion. Initially, the group concentrated on politically driven cyberattacks, but it has since expanded its activities to include ransomware deployment, data leaks, and psychological pressure tactics. By maintaining a structured leak site on the dark web, DragonForce enhances its impact, using public exposure and countdown-driven extortion to pressure victims into compliance.

From a malware analysis perspective, DragonForce demonstrates a high level of technical sophistication. It utilizes the leaked LockBit builder, Zlib-compressed configurations, and evasive deployment techniques. These methods enable the malware to evade security products and configurations, execute targeted process terminations, and ensure efficient file encryption. The group's stealthy execution and obfuscation tactics suggest a well-organized approach that increases the effectiveness of its ransomware operations.

Despite its reputation as a hacktivist group, DragonForce's infrastructure, monetization strategies, and targeting patterns indicate an increasing emphasis on financial gain. The organization's use of darknet platforms and Telegram channels serves dual purposes: promoting its ideology and facilitating operational logistics, thereby solidifying its presence in the cyber threat landscape.

Indicators of Compromise

1. 05f1a39c0902297debceb4c9c4c6674c
2. *.dragonforce_encrypted
3. C:\Users\Public\icon.ico\log.log
4. C:\Users\Public\icon.ico: a0bbc666c39f80d6ac18ae1b253c3462
5. C:\Users\Public\wallpaper_white.png: 07fb997df804901c7f09bcce85ec2c05

6. Mutex: hsfjuukjzloqu28oajh727190

MITRE ATT&CK

Yara Rule

Yara Detection