LockBit Black & DragonForce: Unraveling the Link

By cybleinc

Published: 2024-04-24 · Archived: 2026-04-05 20:38:29 UTC

CRIL investigates DragonForce Ransomware and its links to a leaked LOCKBIT Builder.

Key Takeaways

- Cyble Research & Intelligence Labs (CRIL) identified a DragonForce ransomware binary based on LOCKBIT Black ransomware, suggesting the threat actors behind DragonForce used a leaked builder of LOCKBIT Black ransomware to generate their binary.
- In September 2022, an X (Twitter) user shared the download link for the LockBit ransomware builder, which allows threat actors to customize ransomware payloads according to their preferences.
- A comparison between binaries generated using the Leaked Builder of LOCKBIT ransomware and DragonForce ransomware revealed significant similarities, indicating the DragonForce ransomware binary was likely created using the leaked builder of LOCKBIT ransomware.
- DragonForce ransomware surfaced in November 2023. It utilizes double extortion tactics to target victims, exfiltrating data before encryption and subsequently leaking the data if ransom demands are not met.
- There's also a hacktivist group called DragonForce, based in Malaysia, which claimed to launch their ransomware in 2022. However, it remains unclear whether the group's announced intentions to launch ransomware are connected to the discovered DragonForce ransomware.
- DragonForce ransomware operations began in November 2023 with the public disclosure of victim details on a cybercrime forum and their leak site. To date, they have disclosed information about more than 25 victims worldwide.

Overview

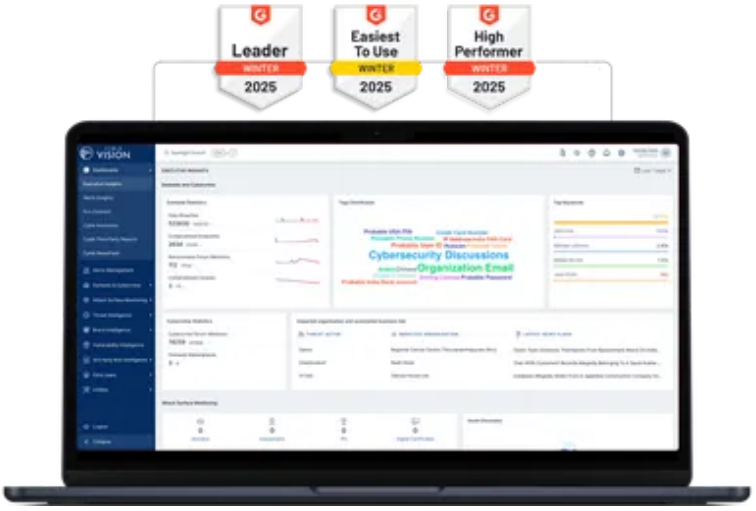
DragonForce Ransomware emerged in November 2023. This group employs double extortion to target its victims, involving data exfiltration followed by encryption. If the victim fails to pay the ransom, the Threat Actors (TAs) behind this ransomware group leak the victim's data on their leak site. The figure below shows the DragonForce ransomware leak site.

Figure 1 – DragonForce Leak Site

There is also a hacktivist group called DragonForce based in Malaysia. During 2021 and 2022, they conducted various campaigns targeting government agencies and organizations across the Middle East and Asia. Additionally, in 2022, the group announced its intention to launch ransomware. However, due to limited information, it is challenging to determine whether the ransomware discovered is connected to this hacktivist group.

See Cyble in Action

World's Best AI-Native Threat Intelligence



DragonForce ransomware began extorting their victims in November 2023 by publishing victim details and their leak site URL on a cybercrime forum. This move was likely aimed at increasing the visibility of their attacks, as only a handful of ransomware groups utilize cybercrime forums for extortion. So far, DragonForce has publicly disclosed information about over 25 victims worldwide. The figure below shows the post on a cybercrime forum.

Figure 2 – Post on Cybercrime Forum

The figure below shows the tor site used for leaking victim's data.

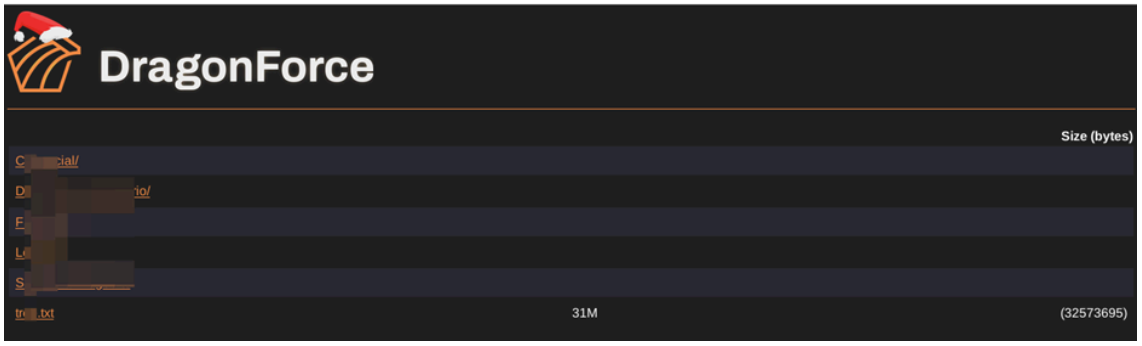


Figure 3 – DragonForce data leak site

CRIL recently found a DragonForce ransomware binary, which was based on LOCKBIT Black ransomware. LOCKBIT Black is a third variant of LOCKBIT ransomware, and we believe that the TAs behind the DragonForce ransomware leveraged the leaked builder of LOCKBIT Black ransomware to generate their binary. The figure below shows the leaked builder of LOCKBIT ransomware.

Figure 4 – Post Regarding Leaked LOCKBIT Builder (Source: Cyble)

On September 2022, a user on X (Twitter) shared the download link of the LockBit ransomware builder. By using this builder, TA can customize the ransomware payload as per their requirements. This builder includes a *"config.json"* file to customize the payload according to the TA's preferences, allowing for features like encryption mode, filename encryption, impersonation, exclusion of specific files and folders from encryption, and language-based exclusion of CIS countries. The configuration file also contains a ransom note template.

Figure 5 – Config.json file of LockBit

Technical Analysis

Our comparison between a binary generated using the Leaked Builder of LOCKBIT ransomware and DragonForce ransomware revealed striking similarities in the code structure and functions. This observation strongly suggests that the DragonForce ransomware binary was likely created utilizing the leaked builder of LOCKBIT ransomware. The figure below shows the BinDiff results.

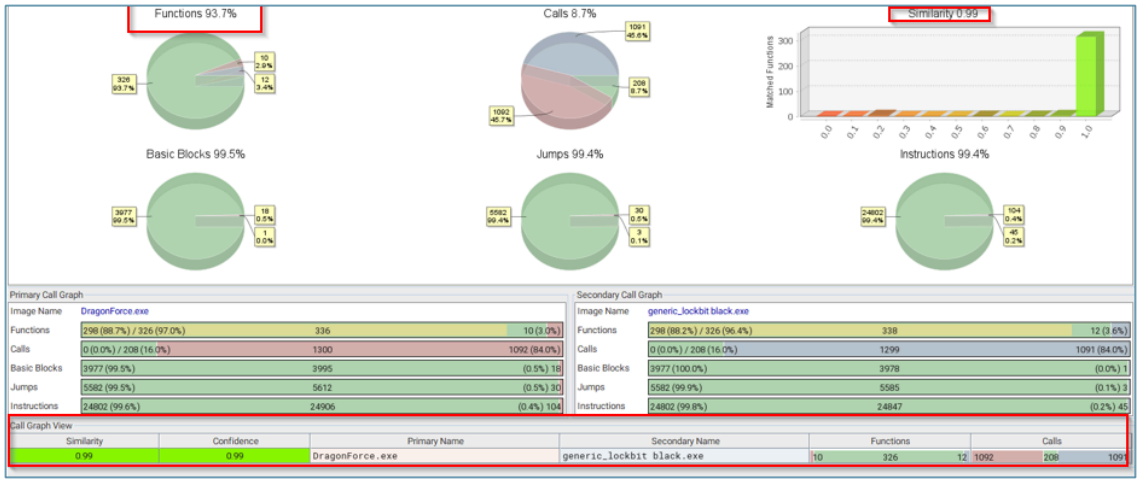


Figure 6 – BinDiff Analysis

Upon execution, the ransomware terminates the following processes to allocate system resources for faster encryption.

oracle	tbirdconfig	powerpnt

ocssd	mydesktopqos	steam
dbsnmp	ocomm	thebat
synctime	dbeng50	thunderbird
agntsvc	sqbcoreservice	visio
isqlplussvc	excel	winword
xfssvccon	infopath	wordpad
mydesktopservice	msaccess	notepad
ocautoupds	mspub	calc
encsvc	onenote	wuauclt
firefox	outlook	onedrive

The ransomware also terminates the following services.

memtas	sophos	GxVss	GxCVD
mepocs	veeam	GxBlr	GxCIMgr
msexchange	backup	GxFWD	NegoExtender

Following encryption, the ransomware binary renames the files using a random string followed by *".AoVOpni2N"* as the extension. The figure below displays the encrypted files.

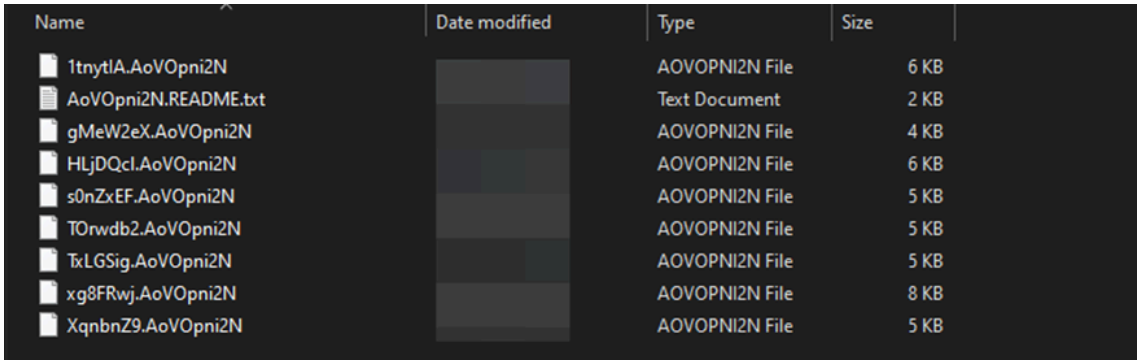


Figure 7 – Encrypted Files

Then, it drops a ransom note named *"AoVOpni2N.README.txt"* in each directory it parses. The figure below displays the ransom note.

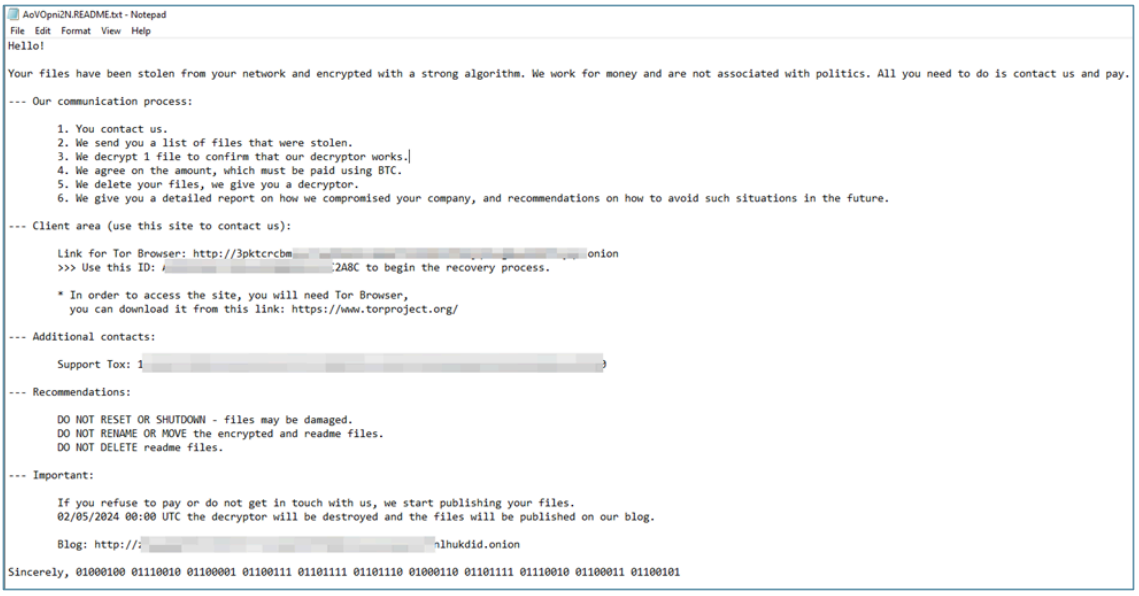


Figure 8 – Ransom Note

A complete analysis of LOCKBIT 3.0 can be found here.

Conclusion

The discovery of DragonForce ransomware and its links to the leaked builder of LOCKBIT Black ransomware underscores the growing threat posed by the abuse of leaked malware-building tools in cyberattacks. The accessibility of such tools enables TAs to customize and deploy ransomware payloads with ease, amplifying the risk landscape for organizations globally. The emergence of DragonForce ransomware, coupled with its utilization of double extortion tactics, highlights the evolving tactics employed by ransomware actors to maximize their impact and financial gain.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

Safety Measures Needed to Prevent Ransomware Attacks

- Do not open untrusted links and email attachments without first verifying their authenticity.
- Conduct regular backup practices and keep those backups offline or in a separate network.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.

Users Should Take the Following Steps After a Ransomware Attack

- Disconnect infected devices on the compromised network.
- Disconnect external storage devices if connected.

- Inspect system logs to check for suspicious events.

Impact of Ransomware

- Loss of valuable data.
- Loss of the organization's reputation and integrity.
- Loss of the organization's sensitive business information.
- Disruption in organization operation.
- Financial loss.

MITRE ATT&CK® Techniques

Tactic	Technique	Procedure
Execution	T1204.002 (User Execution)	Malicious file.
Defense Evasion	T1562.001 (Impair Defenses: Disable or Modify Tools)	Ransomware disables Windows Defender.
Defense Evasion	T1070.004 (Indicator Removal: File Deletion)	Ransomware deletes itself after execution.
Discovery	T1083 (File and Directory Discovery)	Ransomware enumerates folders for file encryption and file deletion.
Impact	T1486 (Data Encrypted for Impact)	Ransomware encrypts the data for extortion.

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
d54bae930b038950c2947f5397c13f84 **e164bbaf848fa5d46fa42f62402a1c55330ef562** **1250ba6f25fd60077f698a2617c15f89d58c1867339bfd9ee8ab19ce9943304b**	MD5 SHA1 SHA256	DragonForce Ransomware

YARA Rule

```
 rule DragonForce{

meta:

   author = "Cyble Research and Intelligence Labs"

   description = "Detects DragonForce Ransomware Memory Strings"
```

```
   date = "2024-04-24"

   os = "Windows"

strings:

   $a1  = ".onion" nocase ascii wide

   $a2  = "Client area" nocase ascii wide

   $a3  = "shadowcopy" nocase ascii wide

   $a4 =  "DO NOT DELETE readme" nocase ascii wide

   $a5 = "encrypted with a strong algorithm" nocase ascii wide

condition:

   all of them

}
```

References

- https://www.radware.com/security/ddos-knowledge-center/ddospedia/dragonforce-malaysia/
- https://cyble.com/blog/alleged-builder-of-lockbit-black-ransomware-leaked/
- https://cyble.com/blog/lockbit-3-0-ransomware-group-launches-new-version/

Source: https://cyble.com/blog/lockbit-blacks-legacy-unraveling-the-dragonforce-ransomware-connection/