New DragonForce Ransomware Emerged from the Leaked LOCKBIT Builder

Date: 01st May 2024 | Severity: High

Summary

A new strain of ransomware called DragonForce has been observed using a leaked ransomware builder from the infamous LockBit ransomware group. The DragonForce ransomware group targets organizations from sectors such as manufacturing, technology, healthcare, finance, construction, and real estate, located in countries like the United States, the United Kingdom, Switzerland, Argentina, and Australia.

Attack Vectors

- Cybersecurity researchers recently revealed that the DragonForce's binary is based on the leaked LOCKBIT Black builder, allowing customization like encryption modes, filename obfuscation, process impersonation, file & folder exclusions, and ransom note templating.
- DragonForce's ransomware binary was created using the leaked builder of the LockBit Black ransomware. Once executed, the ransomware terminates a list of processes and services that might interfere with the encryption (for example, Oracle, Microsoft Office apps, antivirus software, and backup solutions). Then, it encrypts files while appending them with a random string followed by ".AoVOpni2N" as the extension. Finally, a ransom note is dropped in every parsed directory.
- DragonForce operates an active leak site in which it uploads the data of victims who refused to pay the ransom. The leak site contains general data about the victims, and also provides a method to contact the ransomware operators through an internal contact form.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• e164bbaf848fa5d46fa42f62402a1c55330ef562 • d54bae930b038950c2947f5397c13f84 • 1250ba6f25fd60077f698a2617c15f89d58c1867339bfd9ee8ab19ce9943304b
URL	• http://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion/

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Verify links and email attachments before opening.
- Regularly backup data and store it offline.
- Enable automatic software updates on all devices.
- Utilize reputable antivirus and security software.
- Disconnect infected devices from the network.
- Disconnect external storage devices if connected.
- Monitor system logs for suspicious activity.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.tripwire.com/state-of-security/dragonforce-ransomware-what-you-need-know
- https://gbhackers.com/dragonforce-ransomware-lockbit-leak/
- https://www.infosecurity-magazine.com/news/dragonforce-ransomware-lockbit/