May 8, 2025

EMERGING THREATS

DRAGONFORCE RANSOMWARE

DragonForce Ransomware is a malware strain that emerged in 2023 and operates under the Ransomware-as-a-Service (RaaS) model. The group behind DragonForce (under the same name) initially gained attention with politically motivated attacks, targeting entities that aligned with their ideological beliefs. Over time, they have pivoted to financially motivated extortion campaigns, making it a significant player in the ransomware sector. Their operations are structured to allow affiliates to launch attacks using DragonForce's infrastructure and tools, with the ransomware's customizable payloads, allowing affiliates to target a range of industries. As a result, the variant has been associated with a wide array of attacks globally, particularly affecting high-profile targets in the retail, financial, and manufacturing sectors across North America, Europe, and Asia.

THREAT SUMMARY

DragonForce Ransomware is a malware strain that emerged in 2023 and operates under the Ransomware-as-a-Service (RaaS) model. The group behind DragonForce (under the same name) initially gained attention with politically motivated attacks, targeting entities that aligned with their ideological beliefs. Over time, they have pivoted to financially motivated extortion campaigns, making it a significant player in the ransomware sector. Their operations are structured to allow affiliates to launch attacks using DragonForce's infrastructure and tools, with the ransomware's customizable payloads, allowing affiliates to target a range of industries. As a result, the variant has been associated with a wide array of attacks globally, particularly affecting high-profile targets in the retail, financial, and manufacturing sectors across North America, Europe, and Asia.

DragonForce has targeted major companies such as Marks & Spencer, Co-op, and Harrods in the UK, causing significant operational disruptions and reputational damage. In most recent events, The threat group employs a dual-extortion strategy, where after encrypting data, they threaten to release exfiltrated information if the ransom is not paid. This tactic has made the ransomware particularly effective at pressuring victims into compliance, with ransomware demands often exceeding hundreds of thousands of dollars. The group utilizes a white-label RaaS model, which means they offer their ransomware tools to affiliates, giving them a larger pool of potential threat actors to carry out attacks. This expansion of operations has led to a dramatic increase in the number of DragonForce-linked incidents, with affiliates accounting for the bulk of the ransomware deployments. To date, they have claimed responsibility for more than 70 attacks across several countries. As DragonForce continues to evolve its tactics, techniques, and procedures (TTPs), organizations worldwide must prioritize preparation against this growing threat.

TITAN REFERENCES:

TITAN Info Report: Actor koley (aka BackHub, backhub, RansomHub_Team) claims competitors responsible for RansomHub ransomware-as-a-service disruption, reveals plans for recovery

TITAN Info Report: Underground PerspectiveMajor UK retailers M&S, Co-op fall victim to cyberattacks

TITAN Spot Report

HUNT PACKAGE COLLECTION:

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('1dc6b586-95ae-4b89-a1fc-ae6846bd570c'),touched:!t)

SYNOPSIS

DragonForce Ransomware is a sophisticated ransomware strain that has emerged as a prominent threat actor in the community, operating as a Ransomware-as-a-Service (RaaS) and responsible for over 70 attacks globally. DragonForce employs a sophisticated, modular approach to cyber extortion. This modular, customizable platform that affiliates are able to use to execute ransomware attacks, is able to be tailored to their specific target. This flexibility allows DragonForce to scale its operations and effectively penetrate diverse industries. Affiliates can customize payloads for various platforms, including Windows, Linux, ESXi, and NAS systems, using DragonForce's provided affiliate panel. The ransomware utilizes AES-256 and RSA encryption algorithms to lock files, appending the ".dragonforce_encrypted" extension to targeted files. It is also worthy to note that it supports ChaCha8 encryption in newer variants for improved performance.

The group's initial access vectors include phishing emails, exploitation of known vulnerabilities (e.g., CVE-2021-44228 - Log4Shell), and brute-force attacks on exposed services like RDP and VPNs. Once inside, DragonForce deploys tools such as Mimikatz, Cobalt Strike, and SystemBC for credential harvesting, lateral movement, and persistence. It also employs techniques like access token manipulation and process injection to escalate privileges and evade detection . Data exfiltration is conducted via protocols like SFTP and WebDAV, and stolen data is often uploaded to platforms like MEGA or DragonForce's own leak sites.

The DragonForce group's use of encrypted communications, obfuscation techniques, and customized ransomware variants indicates a well-resourced and adaptable threat actor capable of executing large-scale, high-impact cyberattacks. Furthermore, the DragonForce Ransomware variant's continued development, the updating of versioning and added functionalities, makes it very important to assess and prepare for as more information/data become available.

HUNT PACKAGE COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('1dc6b586-95ae-4b89-a1fc-ae6846bd570c'),touched:!t)

RELATED HUNT PACKAGES

SPLASHTOP RMM COMMAND LINE INSTALL

https://hunter.cyborgsecurity.io/details/use-case/d6ea6636-943e-4232-afb7-c67c5ec1c999

AUTORUN OR ASEP REGISTRY KEY MODIFICATION

https://hunter.cyborgsecurity.io/details/use-case/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c

TEAMVIEWER SERVICE INSTALLATION - POTENTIAL REMOTE MANAGEMENT TOOL INSTALLATION

https://hunter.cyborgsecurity.io/details/use-case/30379427-861B-49EC-A107-B0B2BE086A34

DNS QUERY FOR TEAMVIEWER ASSOCIATED DOMAIN BY NON-STANDARD TEAMVIEWER PROCESS NAME - POTENTIAL DEFENSE EVASION

https://hunter.cyborgsecurity.io/details/use-case/C2B6B3E1-8AEA-4AE5-94F1-5505A275A84C

ACTIVE DIRECTORY DISCOVERY AND RECONNAISSANCE - ADFIND.EXE EXECUTION

https://hunter.cyborgsecurity.io/details/use-case/dac3faed-30b5-4e03-aab4-f96eb7b5b3a4

TEAMVIEWER EXECUTION FROM ABNORMAL FOLDER - POTENTIAL MALICIOUS USE OF RMM TOOL

https://hunter.cyborgsecurity.io/details/use-case/01C765B7-10B3-428B-B4F8-594AA90B78E9

TEAMVIEWER BINARY FILE WRITE - POTENTIAL TEAMVIEWER INSTALLATION OR USAGE

https://hunter.cyborgsecurity.io/details/use-case/76E4D345-49D8-4D9A-8335-36999A5CFFB3

ATERA AGENT UTILIZED FOR UNAUTHORIZED REMOTE ACCESS

https://hunter.cyborgsecurity.io/details/use-case/b479f6b2-b14c-4667-be40-6ec310dbd934

POTENTIAL UEFI VOLUME TAMPERING VIA BCDEDIT BOOT CONFIGURATION CHANGES

https://hunter.cyborgsecurity.io/details/use-case/b9ad80ee-ff7c-4829-96d5-2c45e657985b

ANYDESK SILENT INSTALLATION - POTENTIAL MALICIOUS RMM TOOL INSTALLATION

https://hunter.cyborgsecurity.io/details/use-case/11353A3B-797D-45BC-BA32-3D10F14EDC82

REMOTE ATERA AGENT DOWNLOAD - COMMAND LINE

https://hunter.cyborgsecurity.io/details/use-case/bb771c73-e7ab-4705-92a2-ce322b33621d

REMOTE ATERA AGENT DOWNLOAD - WEB

https://hunter.cyborgsecurity.io/details/use-case/7ccc1404-1499-45ba-9c7d-59f42ba321e3

MALICIOUS POWERSHELL PROCESS - CONNECT TO INTERNET WITH HIDDEN WINDOW

https://hunter.cyborgsecurity.io/details/use-case/43c8d198-1def-4530-a35a-569e9ebda53e

ANYDESK PASSWORD SET VIA CLI - POTENTIAL MALICIOUS RMM TOOL INSTALLATION

https://hunter.cyborgsecurity.io/details/use-case/8E0CF375-A8D7-46BD-B9B9-C7181B194706

ANYDESK SERVICE INSTALLATION - POTENTIALLY MALICIOUS RMM TOOL INSTALLATION

https://hunter.cyborgsecurity.io/details/use-case/4103B086-F093-4084-9125-15B9A6C872B8

SHADOW COPIES DELETION USING OPERATING SYSTEMS UTILITIES

https://hunter.cyborgsecurity.io/details/use-case/2e3e9910-70c1-4822-804a-ee9919b0c419

MITRE CONTEXT

- MITRE Tactic Names:
  - Discovery
  - Persistence
  - Command and Control
  - Defense Evasion
  - Impact
  - Execution
  - Privilege Escalation
- MITRE Technique Names:
  - Command and Scripting Interpreter
  - Windows Service
  - Domain Trust Discovery
  - Remote Access Software
  - Inhibit System Recovery
  - Registry Run Keys / Startup Folder
  - Bootkit
- MITRE Technique IDs:
  - T1059
  - T1547.001
  - T1543.003
  - T1542.003
  - T1490
  - T1482
  - T1219
- Threat Names:
  - DragonForce Ransomware

REFERENCES

1. https://hybrid-analysis.blogspot.com/2025/05/shuffling-greatest-hits-how-dragonforce.html
2. https://www.sentinelone.com/blog/dragonforce-ransomware-gang-from-hacktivists-to-high-street-extortionists/
3. https://www.picussecurity.com/resource/blog/dragonforce-ransomware-attacks-retail-giants
4. https://www.group-ib.com/blog/dragonforce-ransomware/