Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

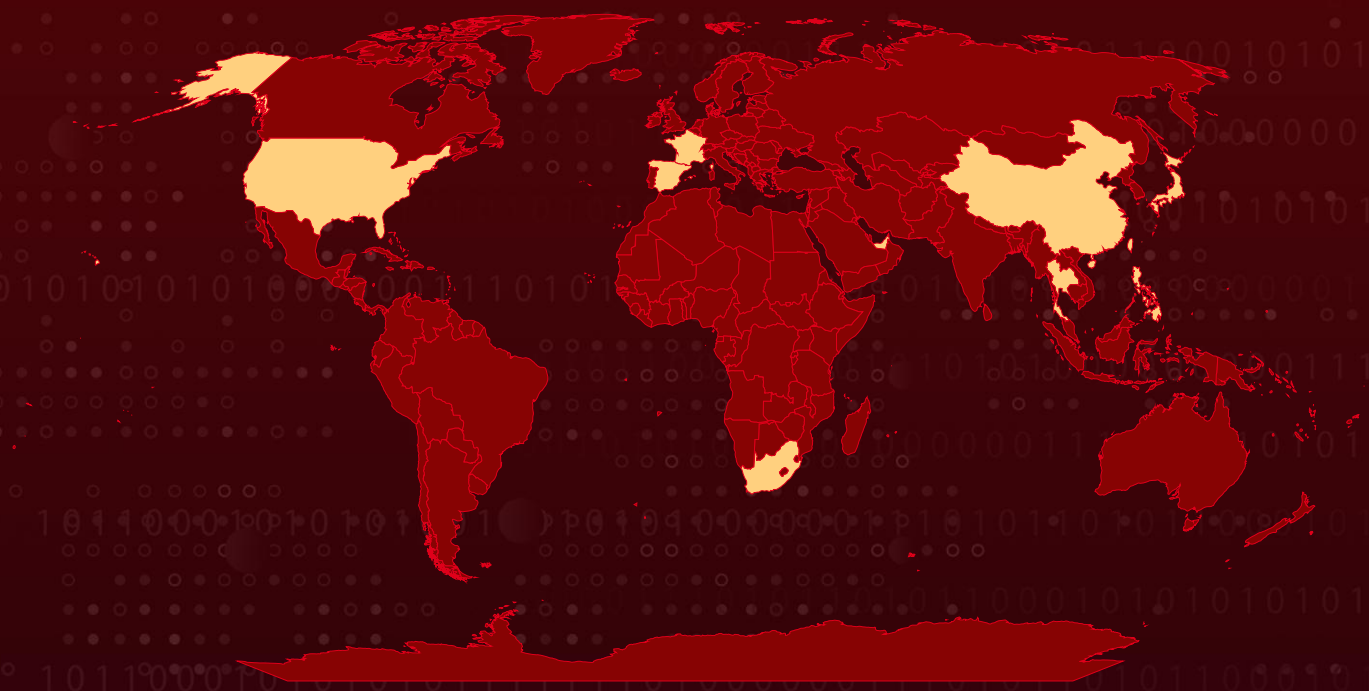
DEVMAN Ransomware Is a New Derivative of the DragonForce Family

Date of Publication	Admiralty Code	TA Number
July 4, 2025	A1	TA2025207

Summary

First Seen: April 2025
Malware: DEVMAN Ransomware
Ransom: $60,000 - $2,500,000
Targeted Countries: China, France, Japan, Philippines, Singapore, South Africa, Spain, Taiwan, Thailand, United Arab Emirates, United States
Targeted Industries: Construction, Electronics, Engineering, Food & Beverage, Government, Healthcare, Human Resources, Manufacturing, Media, Professional Services, Retail, Technology, Transportation
Affected Platform: Windows
Attack: A newly identified ransomware variant, DEVMAN, has emerged from the DragonForce codebase, introducing distinct traits and operational quirks. It is primarily active in Asia and Africa and operates a dedicated leak site known as Devman's Place. Although its operators assert independence, notable code similarities and infrastructure reuse indicate persistent connections within the fragmented Ransomware-as-a-Service landscape.

Attack Regions



Attack Details

#1 DEVMAN is a recently identified ransomware variant built on the DragonForce codebase, featuring unique modifications that point to an independent threat actor. While it reuses much of the original DragonForce framework, it adds its own .DEVMAN file extension and makes subtle behavioral adjustments.

#2 The ransom note text closely mirrors DragonForce's but omits attribution links, reflecting the blurred ownership typical in Ransomware-as-a-Service (RaaS) operations. DEVMAN offers three encryption modes: full, header-only, and custom. DEVMAN operates offline without command-and-control (C2) communication but attempts lateral movement via SMB shares.

#3 On Windows 10, it changes the desktop wallpaper post-infection, a function that fails on Windows 11. A notable flaw is its tendency to encrypt its ransom notes, likely caused by a builder misconfiguration. For persistence, DEVMAN leverages the Windows Restart Manager API, targeting files like NTUSER.DAT while removing registry artifacts, a technique inherited from Conti and DragonForce.

#4 It also uses mutexes and hardcoded synchronization values to prevent reinfection and coordinate file access. The malware avoids certain file types, checks for shadow copies, and renames encrypted files. Ransom notes are always renamed to e47qfsnz2trbkhnt.devman.

#5 DEVMAN has been most active in Asia and Africa, highlighting the chaotic, affiliate-driven nature of the ransomware ecosystem. The group also operates a dedicated leak site, Devman's Place, used to publish stolen data and pressure victims into paying. The DEVMAN ransomware group is actively pursuing access within the UK, France, and Canada, indicating a targeted expansion into these priority regions.

Recommendations

Network and System Hardening: Restrict SMB (Server Message Block) traffic where possible, especially lateral movement via open shares. Disable unnecessary SMB services on endpoints and servers. Limit administrative privileges to essential personnel and apply the principle of least privilege across all systems. Enforce strong network segmentation to isolate critical systems and limit lateral propagation opportunities.

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Backup & Recovery Preparedness: Maintain offline, immutable, and regularly tested backups. Ensure recovery time objectives (RTOs) and recovery point objectives (RPOs) meet business continuity requirements in the event of ransomware deployment.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0007** Discovery
TA0008 Lateral Movement	**TA0009** Collection	**TA0040** Impact	**T1547** Boot or Logon Autostart Execution
T1133 External Remote Services	**T1204.002** Malicious File	**T1204** User Execution	**T1059** Command and Scripting Interpreter
T1053.005 Scheduled Task	**T1053** Scheduled Task/Job	**T1027** Obfuscated Files or Information	**T1070** Indicator Removal
T1135 Network Share Discovery	**T1021.002** SMB/Windows Admin Shares	**T1021** Remote Services	**T1005** Data from Local System
T1486 Data Encrypted for Impact	**T1490** Inhibit System Recovery	**T1657** Financial Theft	**T1012** Query Registry
T1070.004 File Deletion			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	e84270afa3030b48dc9e0c53a35c65aa
SHA1	4a34bbad85312ef34b60818a47f7b5bb8e9a7e26
SHA256	df5ab9015833023a03f92a797e20196672c1d6525501a9f9a94a45b0904c7403, 018494565257ef2b6a4e68f1c3e7573b87fc53bd5828c9c5127f31d37ea964f8
Filename	e47qfsnz2trbkhnt.devman
Mutex	hsfjuukjzloqu28oajh727190
Tox ID	9D97F166730F865F793E2EA07B173C742A6302879DE1B0BBB03817A5A04B572FBD82F984981D
TOR Address	qljmlmp4psnn3wqskkf3alqquatymo6hntficb4rhq5n76kuogcv7zyd[.]onion

Recent Breaches

https://www.dhl.com/th-en/home.html
https://www.lantro.com/
https://www.gmanetwork.com/news/
https://www.pestbusters.com.sg/
https://www.elcaminohealth.org/
https://victim-support.eu/
https://smvthailand.com/
https://premiermeats.co.za/
https://www.investhk.gov.hk/
https://www.chec.bj.cn/
https://www.optimax.com.tw/Portal/index.html
https://www.qilincompany.com/
https://www.doumen.fr/

References

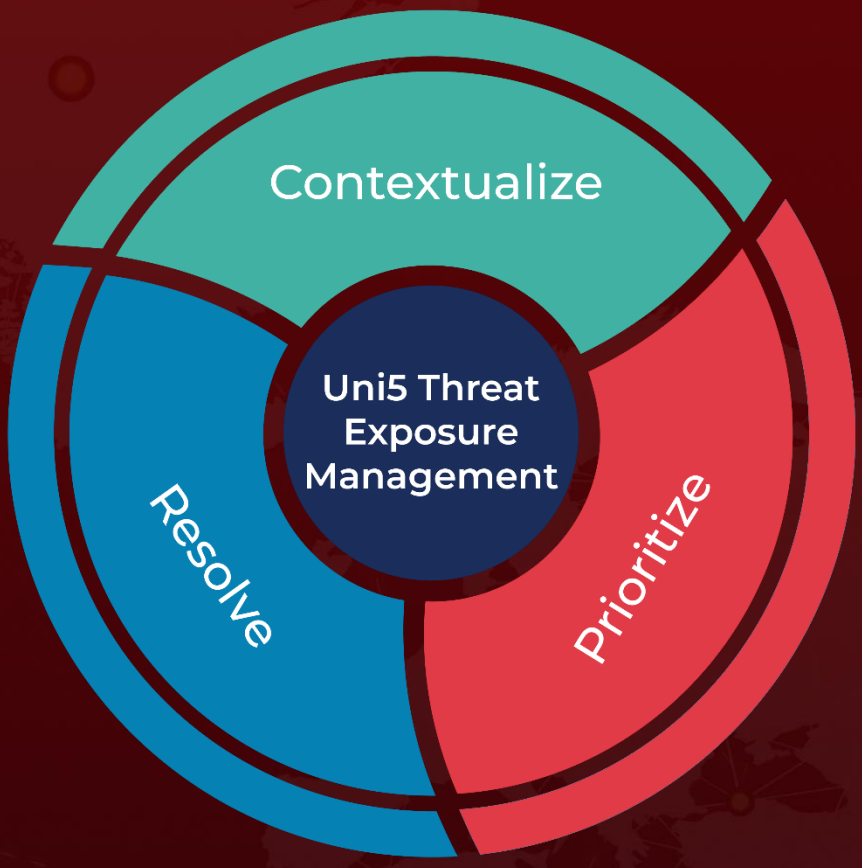
https://any.run/cybersecurity-blog/devman-ransomware-analysis/

https://hivepro.com/threat-advisory/dragonforce-is-selling-diy-ransomware-kits/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 4, 2025 . 5:00 AM

More at www.hivepro.com