21 January 2026

TLP: WHITE

INTEL471

EMERGING THREATS

DevMan Ransomware

DevMan Ransomware is a newly emerging ransomware operation observed in 2025 that has been assessed as a derivative of the DragonForce ransomware family, with researchers also tying its evolution to broader ransomware rebrand patterns seen across ecosystems like Conti and Black Basta. The ransomware has shown an aggressive extortion model that has become more common, impacting organizations with both operational disruption through encryption and added pressure through data theft and leak-site publication. Furthermore, recent analysis highlights DevMan's emergence as part of an increasingly modular ransomware landscape, where operators reuse proven codebases and infrastructure while adjusting naming, branding, and tooling to evade attribution and maintain momentum. This is important to note, because this aligns with the broader trend of ransomware groups shifting identities frequently, while maintaining consistent intrusion behavior and operational playbooks.

THREAT SUMMARY

DevMan Ransomware is a newly emerging ransomware operation observed in 2025 that has been assessed as a derivative of the DragonForce ransomware family, with researchers also tying its evolution to broader ransomware rebrand patterns seen across ecosystems like Conti and Black Basta. The ransomware has shown an aggressive extortion model that has become more common, impacting organizations with both operational disruption through encryption and added pressure through data theft and leak-site publication. Furthermore, recent analysis highlights DevMan's emergence as part of an increasingly modular ransomware landscape, where operators reuse proven codebases and infrastructure while adjusting naming, branding, and tooling to evade attribution and maintain momentum. This is important to note, because this aligns with the broader trend of ransomware groups shifting identities frequently, while maintaining consistent intrusion behavior and operational playbooks.

As far as targeting is concerned, DevMan activity has been reported across multiple regions, with sources noting a strong operational presence affecting organizations in Asia (and additional targeting observed across Africa and Europe). Victimology and reporting indicate the threat has impacted a range of industries, including technology and service sectors, and it presents a high risk to small and mid-sized enterprises due to the speed and disruption ransomware operators can achieve once domain-level access is established. The variant's overall impact includes business downtime, loss of availability for critical systems, exposure of sensitive data, reputational damage, and increased recovery costs, especially when victim environments lack segmentation or resilient backup strategy. DevMan's development and distribution model, along with its lineage ties to other major ransomware families, reinforces that this threat is not isolated and should be treated as part of a larger and continuously evolving extortion ecosystem.

Verity471 Reference:

Info Report: DevMan Attacks Against Healthcare Industry – https://verity.intel471.com/intelligence/infoReportView/report--68eeb2d0-6536-5793-b7fd-7d44e736c465

TITAN Reference:

Info Report: DevMan Attacks Against Healthcare Industry – https://titan.intel471.com/report/inforep/bf66ae54a6110f77587b5c04278a2b9d

SYNOPSIS

DevMan is assessed to be a customized ransomware variant built on the DragonForce codebase, and recent sandbox analysis and threat research highlight that its operators follow a structured intrusion chain consistent with modern human-operated ransomware. Initial access is commonly achieved through compromised credentials, exposed remote services, or other foothold techniques that allow interactive access into the victim environment. Then once inside, operators perform reconnaissance to identify high-value systems, locate shared drives and backups, and determine which hosts are best positioned for maximum impact. DevMan is deployed after attackers obtain sufficient privileges, enabling them to execute encryption broadly across endpoints and network-accessible resources, while maintaining the ability to pressure victims using stolen information and leak-site threats.

When executed, DevMan encrypts targeted files and is associated with a distinct file-extension behavior that supports tracking and victim identification, with reporting noting that it appends a ".DEVMAN" extension to encrypted data. As part of a double-extortion workflow, DevMan operations also emphasize data theft prior to encryption, increasing the likelihood of regulatory exposure and raising the cost of recovery even if restoration is possible. Technical reporting also highlights that DevMan's presence in the ecosystem reflects broader ransomware reuse patterns, where operators repackage and restructure components while retaining the underlying behaviors used for privilege escalation, lateral movement, and mass encryption. This operational design enables DevMan actors to rapidly disrupt business operations, impair system availability, and create sustained pressure for payment through the combined impact of encryption and potential data exposure.

DEVMAN RANSOMWARE COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('19e3dd41-388e-491b-96a8-f5a9bf7d00cc'),touched:!t)

RELATED HUNT PACKAGES

Single-Character Named Files with Execution Extension - Potential Malware Staging

https://hunter.cyborgsecurity.io/research/hunt-package/f20c5f61-c68a-446d-95c4-e227d3ac1078

Autorun or ASEP Registry Key Modification

https://hunter.cyborgsecurity.io/research/hunt-package/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c

Remote Interactive Connections from Unexpected Locations

https://hunter.cyborgsecurity.io/research/hunt-package/e828d24d-e0c6-46aa-8ec3-ed528696276b

Potential Impacket wmiexec Module Command Execution

https://hunter.cyborgsecurity.io/research/hunt-package/5b4c793a-260a-4d43-bbc7-ad4547eeacda

Network SMB Profiling - Potential Nonstandard SMB Communication Behavior

https://hunter.cyborgsecurity.io/research/hunt-package/0fd743e7-f8d1-4f24-b305-6b94db491f47

Possible Impacket service created - smbexec.py module

https://hunter.cyborgsecurity.io/research/hunt-package/d4d0656e-0f6e-40d5-93ba-4f1506a503fa

Unusual Secrets Dump Processes - DonPAPI Activity

https://hunter.cyborgsecurity.io/research/hunt-package/e8b2ffcb-0f64-48c3-853e-5dd0a2be0eee

MITRE CONTEXT

- MITRE Tactic Names:
  - Persistence
  - Execution
  - Credential Access
  - Lateral Movement
  - Collection
  - Command and Control
- MITRE Technique Names:
  - Remote Services
  - Registry Run Keys / Startup Folder
  - Exploitation for Client Execution
  - Ingress Tool Transfer
  - SMB/Windows Admin Shares
  - Service Execution
  - Credentials from Password Stores
  - Windows Remote Management
  - Windows Credential Manager
  - Command and Scripting Interpreter
  - Local Data Staging
  - Windows Management Instrumentation
  - Credentials in Registry
- MITRE Technique IDs:
  - T1105
  - T1203
  - T1021.006
  - T1021
  - T1074.001
  - T1555.004
  - T1569.002
  - T1547.001
  - T1047
  - T1021.002
  - T1552.002
  - T1555

    - T1059
- Exploitation Vulnerabilities:
    - CVE-2024-3400
    - CVE-2025-31324
    - CVE-2024-43451
    - CVE-2023-23397

REFERENCES

1. https://medium.com/@anyrun/devman-ransomware-overview-32600d4da684
2. https://www.halcyon.ai/threat-group/devman#techniques
3. https://www.securonix.com/blog/securonix-threat-labs-monthly-intelligence-insights-july-2025/
4. https://www.vectra.ai/blog/from-conti-to-black-basta-to-devman-the-endless-ransomware-rebrand
5. https://www.hivepro.com/threat-advisory/devman-ransomware-is-a-new-derivative-of-the-dragonforce-family/