

ANY.RUN Releases Technical Analysis of DEVMAN Ransomware Built on DragonForce RaaS

DUBAI, DUBAI, UNITED ARAB EMIRATES, July 1, 2025

/EINPresswire.com/ -- [ANY.RUN](#), a trusted provider of cybersecurity solutions, has published a new technical analysis revealing a ransomware variant that blends traits of DragonForce and Conti families with indicators of a newer actor known as DEVMAN.

Summary: A new ransomware variant, DEVMAN, has been identified. It is built on the DragonForce RaaS framework and exhibits characteristics of the Conti family. The analysis reveals its unique encryption and file handling techniques.

DEVMAN is a relatively new actor that has recently emerged under this name, featuring its own Dedicated Leak Site (DLS) called Devman's Place, a separate infrastructure, and nearly 40 claimed victims, primarily in Asia and Africa, with occasional incidents in Latin America and Europe.

Key findings from the analysis include:

The analyzed sample, initially labeled as DragonForce by antivirus engines, was revealed to be a lightly modified build. It appends the ".DEVMAN" extension to encrypted files, scrambles filenames using a deterministic function, and, due to a builder flaw, encrypts its own ransom notes before victims can read them.

Additional observations from the analysis:

- **Network Activity:** No external C2 traffic was detected; all behavior is confined to the local system.



- [Sample](#) [sample](#): The sample attempts to access hardcoded SMB shares such as ADMIN\$.
- [Mutexes](#) [mutexes](#) [mutexes](#): The use of mutexes and the Windows Restart Manager mirrors tactics from Conti and DragonForce campaigns.

To explore the full technical breakdown and see how DEVMAN behaves inside the sandbox, [visit the ANY.RUN blog](#).

[ANY.RUN](#) [ANY.RUN](#)

ANY.RUN offers a comprehensive suite of cybersecurity solutions, including their Interactive Sandbox and advanced Threat Intelligence services. Trusted by over 15,000 companies worldwide, ANY.RUN enables dynamic malware analysis across Windows, Linux, and Android systems.

In addition to sandboxing, ANY.RUN provides Threat Intelligence Lookup, Feeds, and YARA Search, helping security teams detect, investigate, and respond to threats with greater speed and accuracy.

The ANY.RUN team

ANYRUN FZCO

+1 657-366-5050

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/827298083>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.