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.

□□□□□□□: □ □□□ □□□□□□□ □□□□□□ □□□□□□□□□□ □□□□□□□□□□□□□

DEVMAN is a relatively new actor 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.

□□□□□□□ □□□□□□□□□□□: □ □□□□□□□ □□□□□□□

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.

□□□ □□□□□□□□□ □□ □□□ □□□□□□□ □□□□□□□□□ □□□□□□□□:

· □□□□□ □□□□□□□□□□: No external C2 traffic was detected; all behavior is confined to the local system.

· □□□ □□□□□□□□: The sample attempts to access hardcoded SMB shares such as ADMIN$.

· □□□□□-□□□□□ □□□□□□□□□□□□: 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 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
