EINPRESSWIRE

ANY.RUN Shares Technical Analysis of Mamona, a New Offline Ransomware Strain

DUBAI, DUBAI, UNITED ARAB EMIRATES, May 8, 2025 /EINPresswire.com/ -- ANY.RUN, a trusted provider of cybersecurity solutions, has published a new malware analysis uncovering Mamona, a new commodity ransomware strain that operates entirely offline. The research, conducted by guest contributor Mauro Eldritch, offensive security expert and threat intelligence analyst, reveals how Mamona uses fake extortion tactics, custom encryption, and local execution to evade detection while still encrypting victims' files.

□□□□□□ □□□□□□□□□□ □□□□ □□□□□□ □□□□□□□

Mamona is part of a growing trend in commodity ransomware; malware created with builder kits and distributed without structured affiliate programs. Recently spotted in campaigns linked to the BlackLock group and loosely connected to Embargo, Mamona skips network communication altogether, relying on local execution to encrypt files and pressure victims.

□□-□□□□□ □□□□□□□□ □□ □□□□□□

Key findings of Mamona technical analysis include:

· □□□□□□□□ □□□□□□: Mamona is a newly identified commodity ransomware strain.

· □□ □□□□□□□□ □□□□□□□□□□□□□: The malware operates entirely offline, with no observed Command and Control (C2) channels or data exfiltration.

· □□□□□ □□□□□□□□□□ □□□□: All cryptographic processes are executed locally using custom routines, with no reliance on standard libraries.

· □□□□□□□□□□ □□□□□ □□□□□□□□□: A ping to 127[.]0.0[.]7 is used as a timing mechanism, followed by a self-deletion command to minimize forensic traces.

· □□□□□ □□□□□□□□□ □□□□□□: The ransom note threatens data leaks, but analysis confirms there is no actual data exfiltration.

· □□□□ □□□□□□□□□□ □□□□□□□□: User files are encrypted and renamed with the .HAes extension; ransom notes are dropped in multiple directories.

· □□□□□□□□□□ □□□□□□□□□: A working decryption tool was identified and successfully tested, enabling file recovery.

· □□□□□□□□□□, □□□□□□□ □□□□ □□□□□□: The decrypter features an outdated interface but effectively restores encrypted files.

To explore the full technical breakdown and see how Mamona behaves inside interactive sandboxes, visit the ANY.RUN blog.

□□□□□ □□□.□□□

ANY.RUN offers a comprehensive suite of cybersecurity products, including an interactive sandbox and a Threat Intelligence portal. Trusted by over 500,000 professionals globally, the sandbox provides an efficient and user-friendly service for analyzing malware targeting Windows, Linux and Android systems. Additionally, ANY.RUN's Threat Intelligence services, Lookup, Feeds, and YARA Search, enable users to gather critical information about threats and respond to incidents with better 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/810270150

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.