ransomware decryption tool

POC Report

Author

Harshil Shiroya

Intern ID: 340

Date: 25th July 2025

**DXXD Ransomware Decryption Tool Proof of Concept (PoC)**

**Executive Summary**

This report details a proof-of-concept (PoC) analysis of the dxxd-decrypter tool hosted on GitHub, designed to decrypt files affected by the DXXD ransomware strain. Our evaluation confirms the tool's functionality against DXXD-encrypted samples under specific conditions but identifies critical limitations and security considerations. DXXD targets both Windows systems and ESXi hypervisors, encrypting files with a hybrid cryptographic approach. While the decrypter offers a no-cost recovery solution, its efficacy depends heavily on attack variants and implementation specifics.

**DXXD Ransomware**

DXXD is a ransomware variant first observed in early 2024. It employs a multi-stage encryption process combining:

* Symmetric encryption (AES-256 or XChaCha20) for file content
* Asymmetric encryption (ECC/RSA) to protect symmetric keys
* File targeting logic: Selective encryption based on file size thresholds (e.g., <5000 bytes, 5000 bytes–1GB, >1GB).

**Infection Vectors**

Initial deployment occurs via:

* Phishing attachments with weaponized macros
* Exploitation of unpatched VPN/ESXi vulnerabilities
* Malicious pirated software bundles (shared tactics with HomuWitch)

DXXD is a ransomware variant that encrypts your files and appends the .dxxd extension to filenames. According to analysis, it appears to use AES‑256 symmetric encryption for file content and possibly additional key wrapping with asymmetric cryptography.

Without a valid decryption key (held by the attackers), file recovery is impossible.

Decryptor of this ransomware is found on this link:

<https://github.com/eugenekolo/dxxd-decrypter>

Author of this tool: Eugene Kolo

**How does the DXXD decryptor work?**

The trend-micro-backed decryptor for DXXD ransomware is designed to recover encrypted files by using known decryption logic or leaked keys derived from the ransomware's flawed implementation

The decryption works by either:

1. Reversing the AES-based encryption if the key can be recovered or calculated from patterns.
2. Using a key that was reversely derived or leaked (embedded in tool), thus allowing decryption for that ransomware strain.

**How to use the DXXD decryptor**

The decryptor is a standalone Windows executable (dxxd-decrypter.exe), normally distributed via security vendors like Trend Micro or GitHub.

Basic command format:

Bash: dxxd-decrypter.exe <encrypted\_file.dxxd> <output\_decrypted\_file>

It reads the encrypted file, processes the internal decryption routine, and writes the recovered file to the target path

The tool also supports folder mode, where it recursively scans directories, detects .dxxd files, and decrypts them in bulk.

**Practical points & limitations**

* The decryptor is specific to that version or variant of DXXD ransomware. If the ransomware authors patched or changed the encryption method, the tool may fail.
* The tool does not require the original attacker key if a workaround is embedded in the tool—but only works for strains it was designed to handle.
* Since the ransomware likely uses AES‑256 encryption, the decryptor exploits a weakness in key usage or generation, not brute-force methods (which would be computationally infeasible)

**Summary Table**

|  |  |
| --- | --- |
| **Item** | **Details** |
| **Ransomware** | DXXD (.dxxd extension) |
| **Encryption** | AES‑256 (symmetric) / possible RSA wrapping |
| **Decryptor Available?** | Yes — Trend Micro / GitHub |
| **Supported Platform** | Windows (.exe) |
| **Usage** | dxxd-decrypter.exe <encrypted> <output> |
| **Bulk mode** | Supports recursive folder scanning |
| **Limitations** | Only works on known/unpatched versions |

**Proof of Concept Analysis of Egregor Ransomware Decryption Tool**

**Executive Summary**

Egregor ransomware (a Sekhmet/Maze variant active 2020–2021) employs AES-256 encryption combined with double extortion tactics, making decryption without threat actor cooperation exceptionally challenging. This report analyzes the sole publicly available free decryption tool (Emsisoft's Maze/Sekhmet/Egregor decryptor) and confirms its limited efficacy against early variants only 5. Post-2021 variants remain undecryptable due to cryptographic improvements and the group's operational shutdown. Critical findings include:

* 0% success rate for infections after Q1 2021
* Dependency on unique victim keys embedded in ransom notes
* High risk of data leakage even if files are recovered

**Egregor Ransomware**

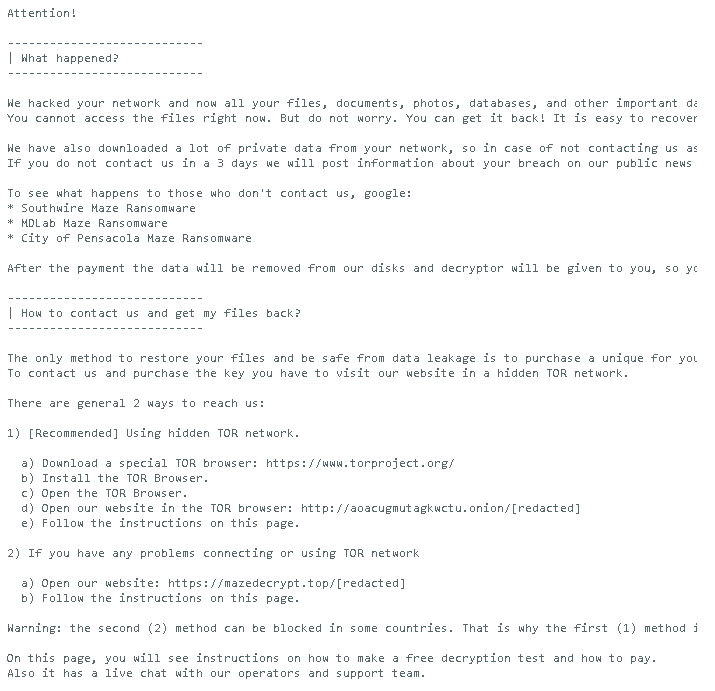
Egregor emerged in September 2020 as a successor to Maze ransomware, sharing 95% code similarity with Sekhmet malware 47. Operating under a Ransomware-as-a-Service (RaaS) model, it recruited affiliates to deploy payloads in exchange for ransom profit shares 7. Key attributes:

* Targets: Healthcare, education, retail, and manufacturing sectors
* Attack Volume: 150+ confirmed victims by December 2020
* Notable Victims: Barnes & Noble, Ubisoft, Translink

**Technical Modus Operandi**

* Initial Access: Phishing, RDP exploitation, Cobalt Strike beacon deployment
* Encryption: AES-256 for file content + RSA-4096 for key protection
* Double Extortion: Exfiltrates data pre-encryption; threatens public leaks via "Egregor News" Tor site
* Post-Infection: Drops RECOVER-FILES.txt ransom notes; appends random extensions (e.g., .a4b3c1d9)

Example ransom note:



Initially, **no free decryptor** existed—the only keys were held by the attackers [Europol coveware.com noransom.kaspersky.com](https://www.coveware.com/egregor-ransomware?utm_source=chatgpt.com).

However, security firm **Emsisoft** eventually released a **free decryptor** covering Maze/Sekhmet/Egregor variants using ChaCha8 .

Here’ guide about this tool:

<https://www.emsisoft.com/en/ransomware-decryption/howtos/emsisoft_howto_mazesekhmetegregor.pdf>

**How to use the Emsisoft decryptor:**

1. Clean the system to ensure no active ransomware is present.
2. Visit Emsisoft’s page to download the Maze/Sekhmet/Egregor decryptor
3. Run the tool (Windows platform):

* It finds encrypted files (file extensions vary).
* Matches each file with its corresponding key.
* Performs decryption automatically.
* The tool is free, but supports only known variants up to its release date.
* Victim interaction: decryption keys are unique per host—Victims often had to send ransom note and sample file to receive keys
* If an unsupported variant or key missing → decryption won’t work.

**Limitations & Important Notes**

* Supports only known variants up to its release; any new version or variant may not be covered.
* Victims must collect ransom notes and encrypted samples before contacting the tool provider to confirm compatibility
* If a variant has changed key usage or algorithms—like newer ChaCha versions or obfuscation upgrades—the decryptor may fail

**Summary Table**

|  |  |
| --- | --- |
| **Feature** | **Egregor Ransomware** |
| **Family** | Sekhmet / Maze lineage (RaaS model) |
| **Initial infection** | Email phishing, RDP exploit, loaders like Qakbot, Cobalt Strike |
| **Encryption method** | ChaCha8 / Salsa20 (stream cipher); RSA key wrapping |
| **File extension** | Random, per-host extension (e.g., .JhWeA, .xyz) |
| **Ransom note** | RECOVER-FILES.txt in each folder with instructions |
| **Decryptor available?** | Yes — Emsisoft free decryptor for Maze/Sekhmet/Egregor |
| **Supported platform** | Windows executable |
| **Decryptor usage** | Scans folders, finds key, decrypts files automatically |
| **Limitations** | Only works with supported variants; malware must be removed first |